PRISM MICROSYSTEMS

EventTracker

User's Guide

Copyright

All intellectual property rights in this work belong to Prism Microsystems, Inc. The information contained in this work must not be reproduced or distributed to others in any form or by any means, electronic or mechanical, for any purpose, without the prior permission of Prism Microsystems, Inc., or used except as expressly authorized in writing by Prism Microsystems, Inc.

Copyright © 1999 - 2010 Prism Microsystems, Inc. All Rights Reserved.

Trademarks

All company, brand and product names are referenced for identification purposes only and may be trademarks or registered trademarks that are the sole property of their respective owners.

Disclaimer

Prism Microsystems, Inc. reserves the right to make changes to this manual and the equipment described herein without notice. Prism Microsystems, Inc. has made all reasonable efforts to ensure that the information in this manual is accurate and complete. However, Prism Microsystems, Inc. shall not be liable for any technical or editorial errors or omissions made herein or for incidental, special, or consequential damage of whatsoever nature resulting from the furnishing of this manual, or operation and performance of equipment in connection with this manual.

PRISM MICROSYSTEMS

Contents

About this Guide x
Purpose of this guide x
Who should read this guide x
Typographical Conventions x
Document Revision Control xi
How to Get In Touch xii
Documentation Support xii
Customer Support xii
Chapter 1 Getting Started 13
About EventTracker 14
EventTracker Services and Ports 16
Starting EventTracker 18
Control Panel 20
Management Console User Interface 25
Event-O-Meter 27
EventTracker Icons 28
Upgrading EventTracker Manager License 29
Accessing About EventTracker console 30
EventTracker Components 33
System Manager 33
EventVault Warehouse Manager 35
Events Knowledge Base 37
EventTracker Diagnostic & Support Tool 37
Chapter 2 EventTracker Management Console 40
Choosing Columns 41
Search Based Console 41
Filtering Events from View 43
Configuring Event Filters 44
Modifying Event Filter settings 50
Deleting Event Filters 51
Configuring Event Filters with Exception 51
Understanding Filters and Filter Exceptions 55
Viewing and Editing Alert Details 56
Reloading the Navigation Pane 58
Auto Scrolling Option 61
Printing Current View Event details 62
Chapter 3 Configuring Manager 63
Setting the Window View Limit (Console) 64

EventTracker Knowledge Base Web site 64
SYSLOG Receiver 65
Monitoring Syslogs 65
Virtual Collection Points 66
VCP Architecture 66
Configuring EventTracker Receiver to listen on multiple ports 67
Virtual Collection Points for Syslogs 68
Configuring EventTracker Receiver Ports 68
Forwarding Raw Syslog messages 70
Virtual Collection Points for Windows Events 71
Example Scenario 71
Computer: Sys1 – Configuring Ports 71
Upgrading Agent (Sys2) from Manager (Sys1) 75
Upgrading Agent (Sys3) from Manager (Sys1) 75
Configuring Correlation Receiver 76
Direct Log File Archiving 76
Enabling Alert Notification Status Tracking 77
Purging Alert Events Cache 77
Show Only Active Alert events in Console 78
Store Only Active Alert events 78
Enabling Remedial Actions 79
Suppressing Duplicate Alerts 80
What does "Duplicate Alert Suppression" mean? 80
How do I use the feature "Duplicate Alarm Suppression"? 80
Configuring Manager to Alert Suspicious Network Activity 81
Chapter 4 Configuring Alerts and Alert Notifications 84
Alerts 85
Configuring Alerts 85
Managing Categories 97
Modifying Alert Details 103
Deleting Alert Details 104
Configuring Alert Actions – Manager Side 105
Configuring Audible Alert Action 105
Configuring E-mail Alert Action 108
Configuring Console Message Alert Action 112
Configuring RSS Alert Notification 114
Forwarding Events as SNMP Traps 116
Forwarding Events as SYSLOG Messages 118
Executing Remedial Action at EventTracker Manager Console System 121
Editing Alert Actions 123
Executing Remedial Action at EventTracker Agent System 126
Configuring Alert Actions for predefined Alerts 129
Adding Alerts from the Dashboard 130
Chapter 5 Configuring RSS Feeds 132
RSS Feeds 133
Adding RSS feeds 133
Deleting RSS Feeds 136
Chapter 6 Maintenance Tools 139
Creating Index for Archive Files 140
Compacting the Database size 142
Chapter 7 Managing System Groups 146

Discover Modes 147
Auto Discover Mode 147
Manual Mode 147
Adding Computers 148
Adding a single Computer 148
Adding a group of Computers 150
Adding a group of Computers from an IP subnet 152
Removing Computers 155
Removing Computers – Auto Discover Mode 155
Removing Computers - Manual Mode 157
Removing Unmanaged Systems 158
Logical System Groups 163
Creating a New Logical Group - System Type 163
Creating a New Logical Group – IP Subnet 167
Creating a New Logical Group – Manual Selection 169
Modifying a Group 172
Deleting a Group 175
Changing System Type 177
Chapter 8 Managing Windows Agents 180
Agent for Windows Systems 181
Pros 181
Cons 182
Deploying Agents 182
Pre-installation Procedures 182
Installing Windows Agents 182
Uninstalling Windows Agents 191
Upgrading Windows Agents 194
Removing Windows Agent Components 198
Switching Windows Agent Modes 200
Viewing Agent Status 204
Starting the Agent Service 204
Editing Admin Account 204
Generating System Report 207
Managed System Report 208
Unmanaged System Report 209
All System Report 209
Vista Agent 209
Event Publishers in Windows Event Log 209
Event Logs and Channels in Windows Event Log 210
Event Consumers in Windows Event Log 210
Prerequisites 210
Installing / Uninstalling Vista Agent 211
Filtering Events 211
Monitoring EVTX Logfiles 212
Configuring Windows Agent 213
Accessing the Agent Configuration Window 213
Basic configuration 214
Forwarding Events to Multiple Destinations 215
Event Delivery modes 218
Modifying Event delivery modes 218
Removing Managers 220
Filtering Events 221
Filtering Events with Exception 225
Filtering Events with Advanced Filters 227

Enabling SID Translation....230
Enabling High Performance mode....231
Monitoring System Health....232
USB Exception List....235
Monitor Applications....238
Filtering applications that need not be monitored....240
Filtering applications that need to be monitored....241
Monitoring Services....242
Filtering Services that need not be monitored....244
Monitoring Logfiles....245
Viewing File Details....254
Deleting Log file monitoring settings....255
Searching Strings....255
Monitoring Check Point Logs....257
Monitoring VMware Logs....261
Monitoring Network Connections....264
Excluding Network Connections from monitoring....267
Including Network Connections for monitoring....271
Suspicious Connections....273
Monitoring Suspicious Connections....273
Adding programs to the trusted list....278
Adding Firewall Exceptions to the Trusted List....279
Monitoring Processes....280
Removing processes from List of Filtered Processes....282
Maintaining Log Backup....283
Viewing Logs....285
Applying Configuration Settings to Specified Agents....286
Backing up Current Configuration....289
Protecting the Current Configuration Settings....290
Enabling Remedial Action....292
Windows Agent Management Tool....292
Accessing Agent Management Tool....292
Querying Agent Service status - System....293
Querying Agent Service status - Group....294
Querying Agent Service status - All....295
Restarting Agent Service - System....295
Restarting Agent Service - Group....296
Restarting Agent Service - All....296
Querying version of the Agent Service - System....297
Querying version of the Agent Service - Group....297
Querying version of the Agent Service - All....298
Deploying Windows Agents in Command line mode....298
Command line parameters....298
Installing Agent on a single system....299
Uninstalling Agent from a single system....301
Installing and Uninstalling Agents in multiple systems....301
To uninstall Agents from multiple systems....301
Chapter 9 Agentless Monitoring of Windows Systems....303
Agentless Monitoring....304
Pros....304
Cons....304
Adding Systems for Agent-less monitoring....304
Editing Admin account....310
Chapter 10 EventVault Warehouse Manager....312

EventTracker Scheduler service ... 313
EventTracker Scheduler service – Collection Master Console ... 314
EventTracker Scheduler service – Collection Point Console ... 314
Viewing CAB files ... 314
Configuring EventVault ... 315
Backing up EventVault Data ... 317
Saving EventBox Metadata ... 319
Verifying EventBox Integrity ... 320
Extracting EventBox Data ... 321
Deleting an EventBox ... 321
Moving CAB files ... 322
Appending CAB Files ... 323
Chapter 11 Analysis ... 330
EventTracker Log Search ... 331
Event Traffic Analysis ... 331
Traffic Analysis – View by Category ... 332
Correlating Events ... 333
Traffic Analysis – View by Event Id ... 333
Traffic Analysis – View by Custom Selection ... 335
Traffic Analysis – Keyword Analysis ... 336
Tracking Enterprise Activity ... 340
Analyzing Alerts ... 340
Chapter 12 Managing Category Groups and Categories ... 347
Creating Category Groups ... 348
Adding Categories to a Group ... 352
Modifying Category Groups ... 357
Deleting Category Groups ... 358
Managing Event Categories ... 358
Creating Event Categories ... 359
Modifying Categories ... 365
Deleting Categories ... 369
Deleting Event Details ... 369
Adding Categories as Alerts ... 370
Chapter 13 Export Import Utility ... 373
Export and Import Utility ... 374
Exporting Categories ... 374
Exporting Filters ... 376
Exporting Alerts ... 377
Exporting System Groups ... 379
Exporting Systems ... 380
Exporting Schedule Reports ... 382
Exporting RSS Feeds ... 384
Importing Categories ... 385
Importing Filters ... 387
Importing Alerts ... 390
Importing System Groups ... 392
Importing Systems ... 394
Importing Schedule Reports ... 396
Importing RSS Feeds ... 397
Chapter 14 Collection Point Model ... 400
What is Collection Point model ... 401
Scalability ... 401

Real world scenarios 402
Chapter 15 Collection Master 405
Starting Collection Master Console 406
Viewing Collection Point Details 407
Viewing CAB Status 408
Configuring Collection Master listening port 411
Merging Collection Points – default Archives folder 412
Scenario 1 412
Scenario 2 414
Scenario 3 415
Merging Collection Points – modified Archives folder 416
Scenario 1 418
Scenario 2 422
Requesting CAB files 424
Deleting CAB files 428
Deleting Collection Point Detail 430
Configuring Alerts 432
Chapter 16 Collection Point 434
Starting Collection Point Console 435
Adding Collection Masters 436
Editing Collection Master Settings 440
Deleting Collection Master Settings 441
Viewing CAB Status 442
Sending CAB file(s) to Collection Master(s) 443
Chapter 17 EventTracker Configuration Tracking 449
EventTracker Configuration Tracking Events 450
Chapter 18 TrapTracker 451
Chapter 19 Add-in Software Modules 452
WhatChanged 453
StatusTracker 453
EventLogCentral 454
Evaluation and Purchase 454
Solaris Agent 454
Benefits of Solaris Agent 454
Purchase 455
Appendix – HIPAA 456
HIPAA Compliance Reports 456
User Logon report 456
User Logoff report 456
Logon Failure report 456
Audit Logs access report 456
Appendix – SOX 457
Sarbanes – Oxley Compliance Reports 457
User Logoff report 457
User Logon report 457
Logon Failure report 457
Audit Logs access report 457
Security Log Archiving Utility 457
Track Account management changes 458
Track Audit policy changes 458

Track individual user actions 458
Track application access....458
Track directory / file access....458
Appendix – GLBA....459
GLBA Compliance Reports....459
User Logon report....459
User Logoff report....459
Logon Failure report....459
Audit Logs access report....459
Appendix – Security Reports....460
Security Reports....460
Successful and failed file access....460
Successful logons preceded by failed logons....460
Audit log cleared events by user....460
Invalid logons by date....460
Daily reboot statistics....460
CPU load peaks by computers....460
Account usage outside of normal hours....460
Audit policy history....461
Accounts that were never logged on....461
Administrative Access to Computers....461
File Access by User....462
Hot fixes by Computer....462
Last logon by Domain Controller....462
User Account Locked Out....463
Appendix – BASEL II....464
BASEL II....464
Appendix – FISMA....465
FISMA....465
FISMA Sec. 3505....465
FISMA Sec. 3544....465
Appendix – PCI DSS....466
PCI DSS....466
Glossary....467
Index....471

About this Guide

Purpose of this guide

This guide will enable you to use every option of EventTracker and provides detailed procedures for the same.

Who should read this guide

Intended audience:

- Administrators who are assigned the task to monitor and manage events using EventTracker
- Operations personnel who manage day-to-day operations using EventTracker

Typographical Conventions

Before you start, it is important to understand the typographical conventions followed in this guide:

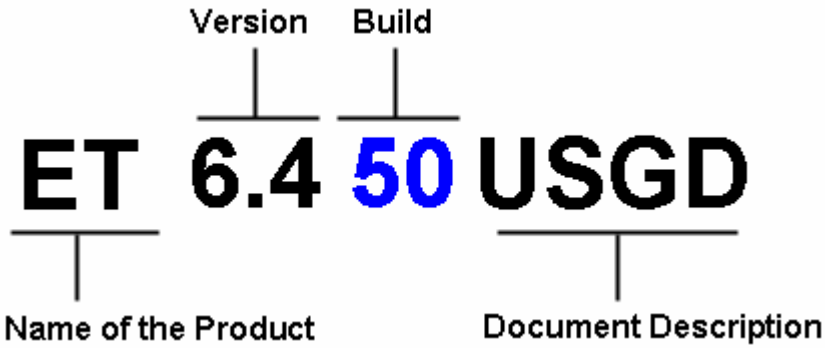
Table 1

This	Represents
Italics	References to other guides and documents.
Bold	Input fields, radio button names, check boxes, drop-down lists, links on screens, menus, and menu options.
CAPS	Keys on the keyboard and buttons on screens.
`{Text_to_customize}`	A placeholder for something that you must customize. For example, `{Server_Name}` would be replaced with the name of your server/ machine name or an IP address.
`Constant width`	Text that you enter, program code, files and directory names, function names.
🗎	A Note, providing additional information about a certain topic.

Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First two letters – name of the product
- Second two numbers – version of the product
- Third two numbers – build of the product
- Last two letters – document description



The document revision control number for this guide is as given below:

Table 2

File Name	EventTracker v6.4 b50 User Guide
Description	Updated in accordance with release version 6.4 build 50.
Status	Final
Release Date	Feb 17, 2010

How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support

Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@prismmicrosys.com

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventTracker, contact us by e-mail at support@prismmicrosys.com. While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
- The type of hardware, including the server configuration and network hardware if available
- The version of EventTracker and the operating system
- The exact message that appeared when the problem occurred or any other error messages that appeared on your screen
- A description of how you tried to solve the problem

Chapter 1
Getting Started

In this chapter, you will learn about:

- Starting EventTracker
- EventTracker Control Panel
- Management Console User Interface
- EventTracker Icons
- Upgrading License
- Accessing About EventTracker Manager Console
- EventTracker Components

About EventTracker

EventTracker framework is Prism Microsystems, Inc's flagship event log monitoring and management product. EventTracker is a reliable and practical software-only solution, to monitor, track and manage critical events that occur in Windows 2000/2003/XP/Vista/2008/MSCS systems and UNIX-style Syslog in your enterprise. Installation of EventTracker is quick, simple, and intuitive. EventTracker comes with a thorough resource kit with several nifty utilities, which alleviates the pain of day-to-day administration of your enterprise network. Log Volume Analysis is similar to Log Analysis but with more bells and whistles, which gives you an incisive insight into the event traffic flow in your enterprise.

EventTracker gives you the ability to:

- **New** Alerts Dashboard.
- **New** Enhanced Enterprise Activity console.
- **New** View and Edit Alert details.
- **New** Search Category based events in the Management Console.
- **New** Store Only Active Alert events.
- **New** Suppress duplicate Alerts.
- **New** Forward events as raw SYSLOG messages.
- **New** Monitor VMware logs.
- Archive event logs for up to 7 years in EventVault(R).
- Configure EventTracker Receiver to listen on multiple ports.
- Configure SYSLOG Receiver to listen on multiple ports.
- Execute Remedial Actions at Agent systems.
- Monitor file transactions that occur in the inserted media (USB or other devices).
- Analyze trend of events through Event-O-Meter.
- Monitor, consolidate, and analyze Windows event log (2000/XP/2003/Vista/2008), Unix/Linux/Cisco SYSLOG, Web sites (http, https), and SNMP based network devices.
- Comply with audit requirements for GLBA, HIPAA, FISMA, Sarbanes-Oxley, California Senate Bill 1386, the USA Patriot Act, NISPOM Chapter 8, and PCI Data Security Standard.
- Deploy Vista Agent.
- Maintain Vista Log Backup.
- Monitor Check Point logs.
- Generate Check Point reports.

- Enable Alert Notification Status Tracking.
- Purge Alert Events Cache.
- Monitor
    - W3C Extended Log.
    - EVTX Log Files.
    - Disk space/Memory/CPU usage.
    - Runaway processes.
    - Device changes.
    - Application install/uninstall.
    - Application usage.
    - Any standard log file.
    - Automatically restart stopped services.
    - TCP/UDP network traffic.
    - Connection states of ports.
- Generate audit reports based on Sites. This feature is available only when you install Collection Master Console.
- Configure Agent to monitor All Network Traffic (NCM) / Suspicious Traffic Only (SNAM).
- Generate Suspicious Network Activity report.
- Enable/disable predefined Trusted Connections List.
- Add programs to Trusted Connections List.
- Add programs and services in Firewall Exceptions list to Trusted Connections List.
- Configure Manager to send notification when there is suspicious traffic in your enterprise network.
- Schedule EventVault™ Integrity check.
- Append Archives through EventVault Warehouse Manager.
- Manage Active Directory (AD) Organizational Units (OU).
- Select agent-based or agentless monitoring.
- Organize event views from SYSLOG and Cisco PIX firewall sources.
- Generate audit-ready compliance reports (HIPAA, SOX, FISMA, GLBA, PCI).
- Configure real-time event alerts via e-mail, beep, RSS Feeds and custom actions.
- Customize views and reports.

- Define report templates.
- Backup and clear event logs automatically.
- Switch Navigation pane refresh modes.
- Reload the Navigation pane with changes made in the System Manager.
- Enable or disable SID translation.
- Switch Agent mode from Standard mode to High Performance mode and vice versa.
- Run 5 reports simultaneously (4 Scheduled Reports and 1 Manual Report).
- Configure
    - Filter Exception in the Filter Events console.
    - Exception Events for Log Analysis.
    - Filters in the generated Log Analysis report to filter the result set.
    - Time based Alerts.
    - Alerts based on Event count.
    - New, modify, and delete Log Volume Analysis schedules.
    - RSS Feeds.
- Analyze
    - Admin user activities.
    - Non-Admin user activities.
    - Alert notification status.
    - Disk space availability, status, and usage variation.

EventTracker Services and Ports

Table 3

Service	Description	Startup Type	Log on as	Allow service to interact with desktop
Event Correlator	Correlates events, and performs rule set based actions.	Automatic	Local System account	Yes

Service	Description	Startup Type	Log on as	Allow service to interact with desktop
EventTracker Agent	Relays local log data. If uninstalled locally, corresponding changes should be made at the Management Console. May be restarted to pick up new configuration.	Automatic	Local System account	Yes
EventTracker Alerter	Sends configured alert notifications - Beep, Email, Message & RSS.	Automatic	Local System account	Yes
EventTracker EventVault	Compresses, and securely stores the raw log data.	Automatic	Local System account	Yes
EventTracker Receiver	Receives log data from the configured sources. If stopped, EventTracker becomes inoperative. May be restarted to pick up new configuration.	Automatic	Local System account	Yes
EventTracker Reporter	Manages report generation.	Automatic	Local System account	Yes
EventTracker Scheduler	Initiates scheduled actions including report generation, log backup etc.	Automatic	Local System account	Yes

Table 4

EventTracker Module	Port(s)
Agent	14506/TCP
Windows Receiver	14505(TCP/UDP) - optional and can be configured up to 10 ports (TCP/UDP)
Syslog Receiver	514(UDP), 1470(TCP) - optional and can be configured up to 10 UDP/TCP port pairs
Receiver (Outgoing)	32001, 32002... up to 32020 (all UDP). Total 20 ports used to send information to EventTracker modules
UserActivity	14556, 14557... up to 14576 (all UDP) to connect 20 Receivers
Correlator	14656, 14657... up to 14676 (all UDP) to connect 20 Receivers
Collection Master	14507/TCP - optional and can be configured to any TCP port
Correlation Receiver	14509/TCP

Starting EventTracker

Search based console helps to search & view events occurred in a specific Category. By default, EventTracker displays number of events as configured in the Manager Configuration window (**Max events view limit (Console)**). Whenever you open the Management Console, EventTracker sets the focus on Correlated Alerts and Incidents Category and displays the events associated with that Category. If there are no events occurred in that particular time frame, EventTracker gives you options to search farther back. You can also configure EventTracker to show/store only the active Alerts through the options provided in the Manager Configuration window.

To start EventTracker

1. Click **Start**, point to **Programs**, point to **Prism Microsystems**, point to **EventTracker**, and select the **EventTracker Management Console** option.

   (OR)

   Double-click **Event Monitoring** on the EventTracker Control Panel.

   EventTracker displays the Splash screen.

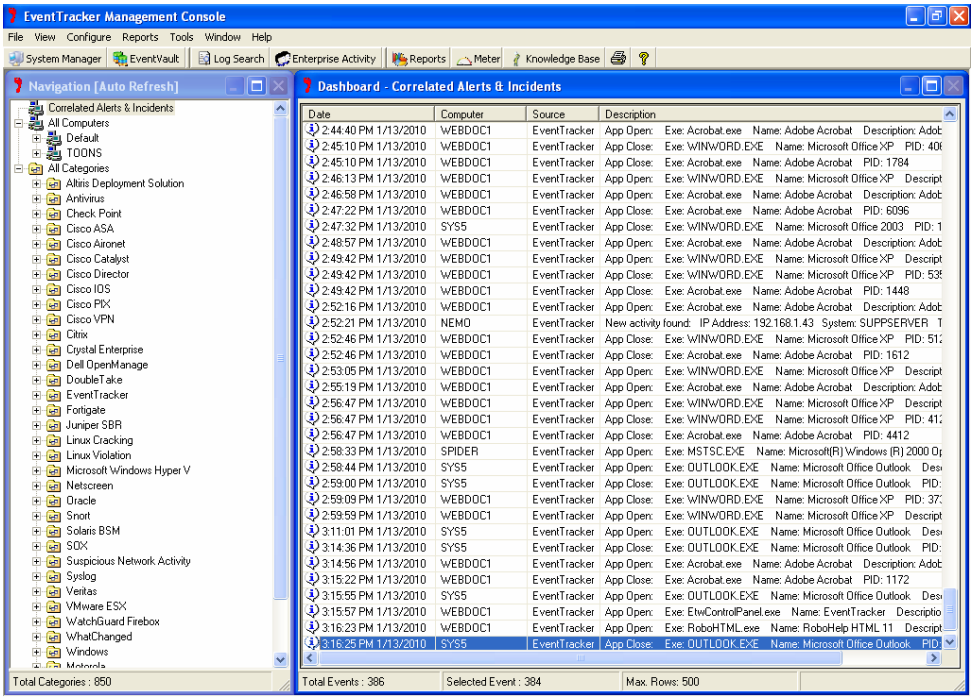
Figure 1 Splash screen

EventTracker displays the Management Console.

Note

After fresh installation of EventTracker, the available agents will be displayed under Default Group in the All Computers hive. To refresh the Navigation pane, open the System Manager and press F5 on your keyboard. The System Manager automatically discovers the Groups and Systems. The **Automatically find and add** option is selected in the Select 'Auto Discover' Mode dialog box. EventTracker displays this dialog box when you open the System Manager for the first time after installing the Event Tracker. If you select the **I will choose to add and track** option, then you have to manually add the Groups. Close the System Manager. Press CTRL+F5 on your keyboard. EventTracker refreshes the Management Console.

Figure 2 Management console



Control Panel

EventTracker control panel consists of shortcuts that help you to quickly access EventTracker components.

To open an application, either double-click (OR) select and press ENTER on your keyboard.

Figure 3 Control Panel – Collection Master

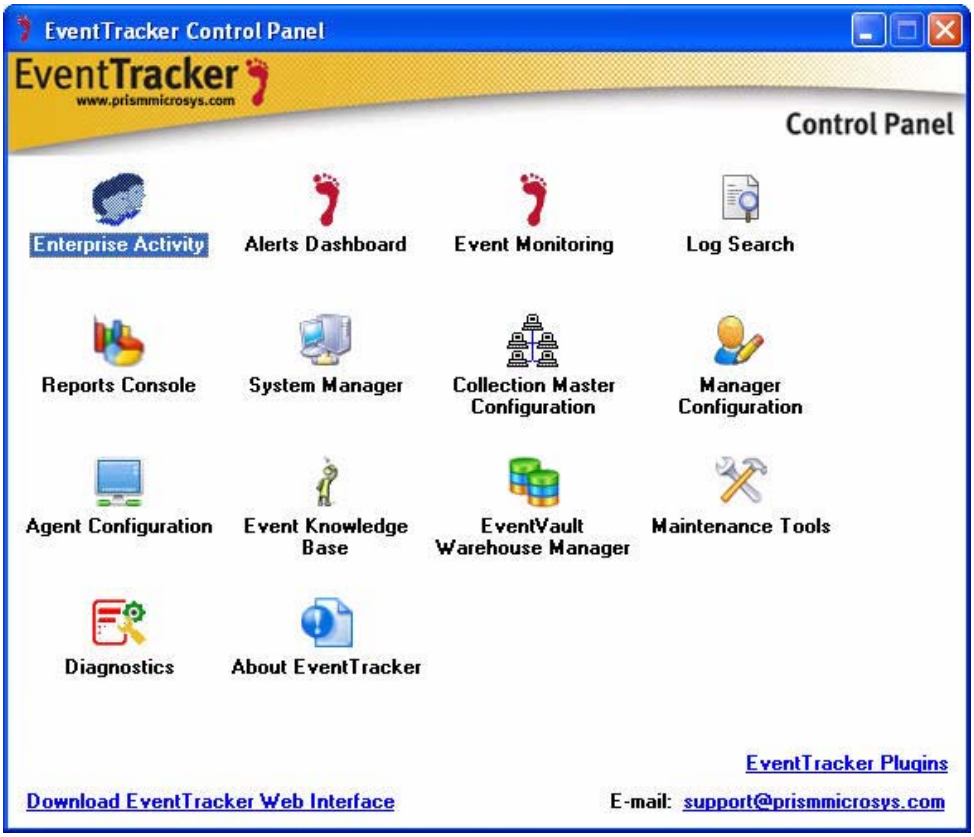


Figure 4 Control Panel – Collection Point

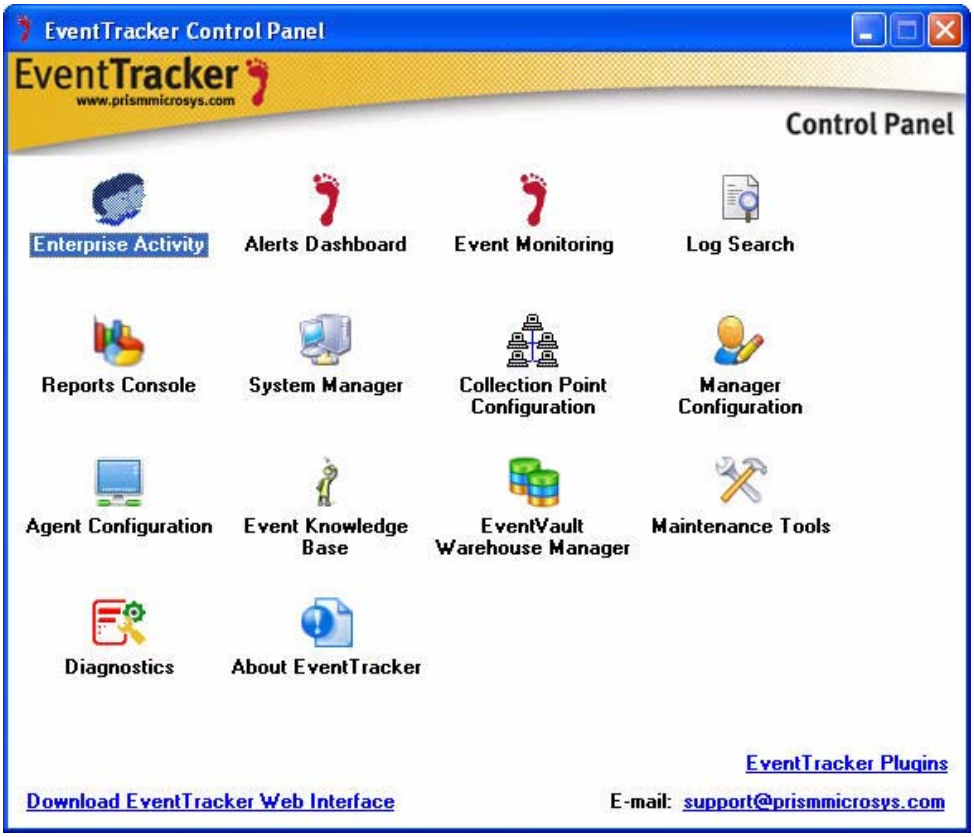


Figure 5 Control Panel – Standard

Table 5

Click	To
Enterprise Activity	Open Enterprise Activity Dashboard.
Alerts Dashboard	Open Alerts Dashboard.
Event Monitoring	Open EventTracker Management Console.
Log Search	Open simplified event log search interface.

Click	To
Reports Console	Open Advanced Reports console.
System Manager	Open System Manager.
Collection Master Configuration	Open Collection Master Configuration console.
Collection Point Configuration	Open Collection Point Configuration console.
Manager Configuration	Open Manager Configuration window.
Agent Configuration	Open Agent Configuration window.
Event Knowledge Base	Go to events Knowledge Base Web site. This Web site provides in-depth details about events.
EventVault Warehouse Manager	Open EventVault Warehouse Manager console.
Maintenance Tools	Open Maintenance Tools window. Archive Indexer — Click to create Index file for Archives. Compaction Utility — Click to compact database.

Click	To
	Click to open Import Export Utility.
	Open Diagnostics tool.
	Open About box.

Management Console User Interface

Management Console is the first component of EventTracker. This section helps you to understand the Management Console user interface. To work with EventTracker effectively, a thorough understanding of its user interface is very important.

Figure 6 Management Console User Interface

Title Bar

The strip at the top of the Management Console is the Title Bar. Title Bar displays the name of the application. You cannot customize, move, or drag the Title Bar.

Menu Bar

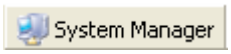
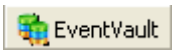
The strip next to Title Bar is the Menu Bar. Menu Bar contains menus. Each Menu contains a list of commands and shortcut keys to carry out a specific task. You cannot customize, move, or drag the Menu Bar.

Toolbar

The third strip is the Toolbar. Toolbar contains command buttons with images. Frequently used options are provided on the Toolbar. You cannot customize, move, or drag the Toolbar.

Mouse over ToolTip for command buttons help you know the purpose the buttons serve.

Table 6

Click	To
	Open System Manager.
	Open EventVault Warehouse Manager.
	Open Log Analysis console.
	Open Enterprise Activity console.
	Open Advanced Reports Console.
	Open Event-O-Meter graph.
	Open EventTracker Knowledge Base Web site. http://kb.prismmicrosys.com
	Print current Events on the Dashboard.

Navigation Pane

Navigation pane displays EventTracker objects such as Computer Groups and Computer in All Computers tree view and Category Groups and Categories in All Categories tree view. You can expand and collapse All Computers and All Categories trees.

Dashboard Pane

By default, EventTracker displays Alert events that occurred in the monitored systems on the Dashboard.

Workspace

The workspace consists of the navigation pane and the dashboard pane.

Status Bar – Navigation pane

EventTracker displays the Total Categories.

Status Bar – Dashboard pane

In the Dashboard pane, EventTracker displays Total Events received since the console is launched in the first section, row id of the selected event in the second section. By default, row id of the latest event is displayed and the Max Rows i.e. the maximum number of events set to view is displayed in the third section. By default, the EventTracker displays 500 rows of events. You reset console view limit in the Manager Configuration window.

Event-O-Meter

Event-O-Meter is an analytical graphical chart that helps quickly visualize per port trends of events against specified time range. In addition, numerical data has also been provided in a tabular format.

Figure 7 Event-O-Meter - Graph

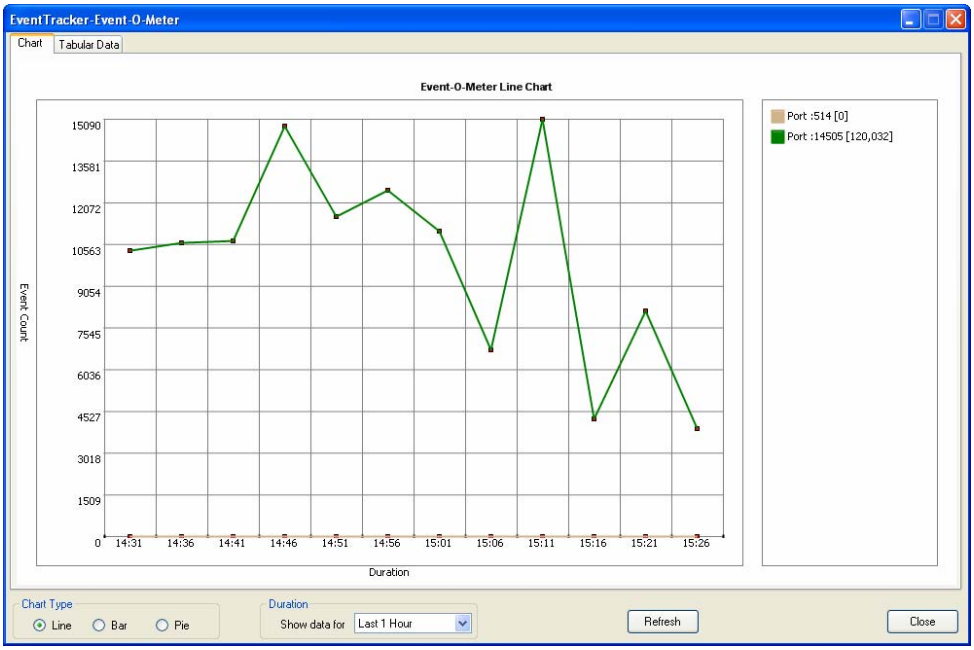
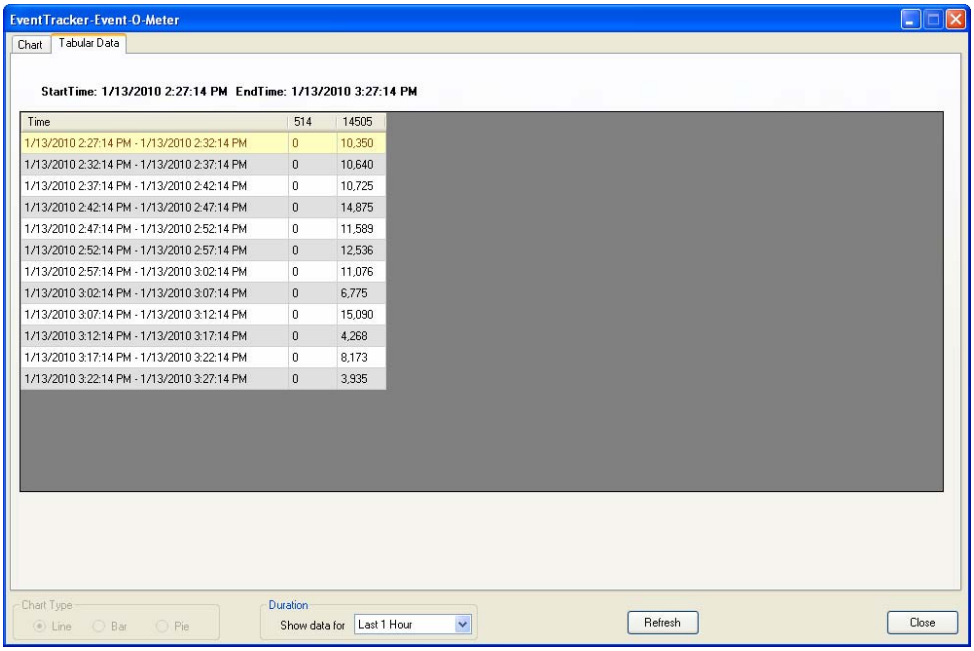


Figure 8 Event-O-Meter - Tabular Data



EventTracker Icons

EventTracker Icons represent EventTracker objects. These icons help you identify various objects used in EventTracker.

Table 7

Icon	Represents
	All computers.
	Computer.
	Category Groups.
	Events of Audit Success Event Type.
	Events of Audit Failure Event Type.
	Events of Information Event Type.
	Events of Warning Event Type.
	View and print the generated report.

Icon	Represents
	Open the Online Help.
	Export the displayed page into Word or PDF file.
	Search a string or phrase in the displayed page.

Upgrading EventTracker Manager License

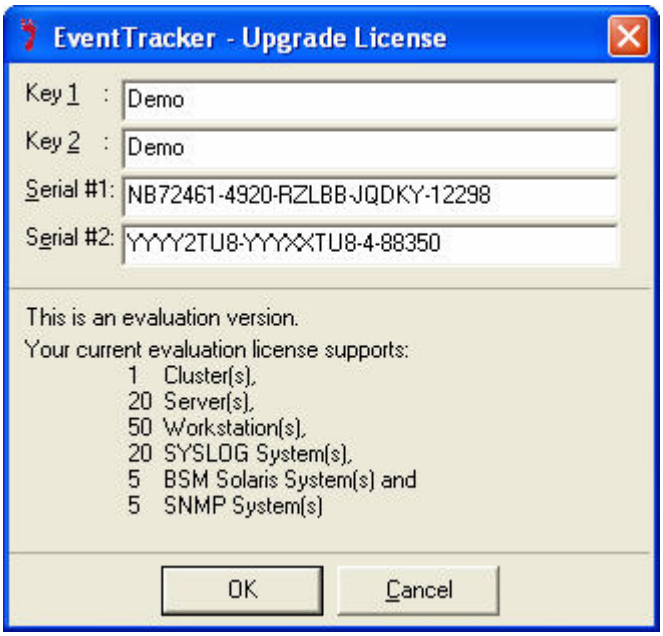
This option helps you upgrade EventTracker Manager license from trial version to registered version.

To upgrade license

1. Open the Management Console.
2. Click the **Help** menu and select the **Upgrade License** option**.**

   EventTracker displays the Upgrade License dialog box.

Figure 9 Upgrade License



Note

You can get the upgrading license information from sales@prismmicrosys.com.

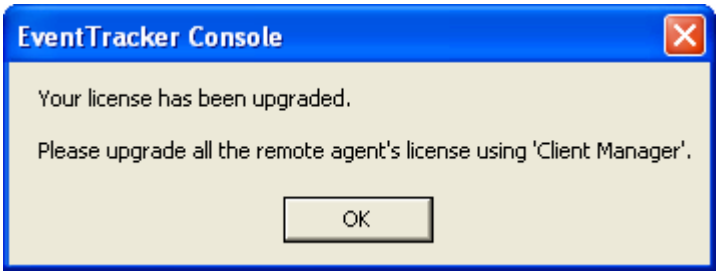
Table 8

Field	Description
Key 1	Type key1 in this field.
Key 2	Type key2 in this field.
Serial #1	Type Serial No.1 in this field.
Serial #2	Type Serial No.2 in this field.

3 Click **OK**.

EventTracker displays the EventTracker Console message box.

Figure 10
EventTracker Console message box


EventTracker Console
Your license has been upgraded.
Please upgrade all the remote agent's license using 'Client Manager'.
OK

4 Click **OK**.

5 Upgrade all remote agents' license as instructed in the message box.

EventTracker displays the EventTracker Console message box.

6 Click **OK**

7 Restart the Management Console.

Accessing About EventTracker console

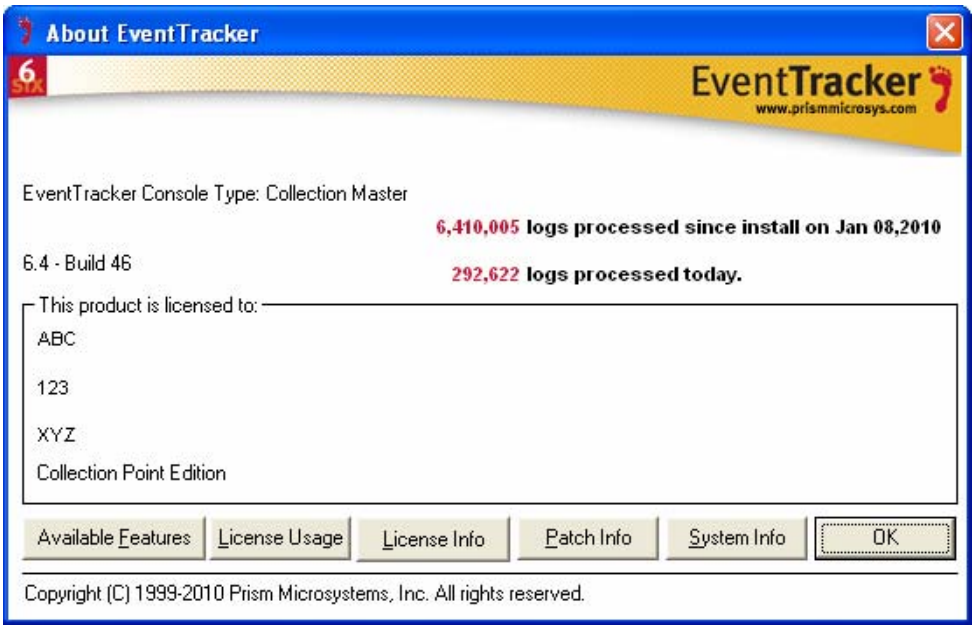
This option helps you view Available Features, License Usage, License Info, Patch Info and System Info.

To access About EventTracker console

1 Double-click **About EventTracker** on the Control Panel.

EventTracker displays the About EventTracker console.

Figure 11 About EventTracker console



2 Click **Available Features**.

EventTracker displays the Available Features window.

Figure 12 Available Features

Available Features - Collection Point Edition
Automatically clear eventlog Available
Backup eventlog Available
Alert - Beep Available
Alert - E-mail Available
Alert - Message Available
Alert - Forward Available
Alert - Custom Available
Alert - RSS Available
Event Reports - Report Console Available
Event Reports - Manage Categories Available
Event Reports - Import Categories Available
Event Reports - Export Categories Available
Event Reports - Quick Statistics Available
Event Reports - Report E-mail Available
Event Warehouse - Manage Archive Available
Event Warehouse - Backup Available
Filter Non-essential events Available
Filter any event(s) for display only Available
Monitor only specific events Available
Filter any specific events Available

3 Click **License Usage**.

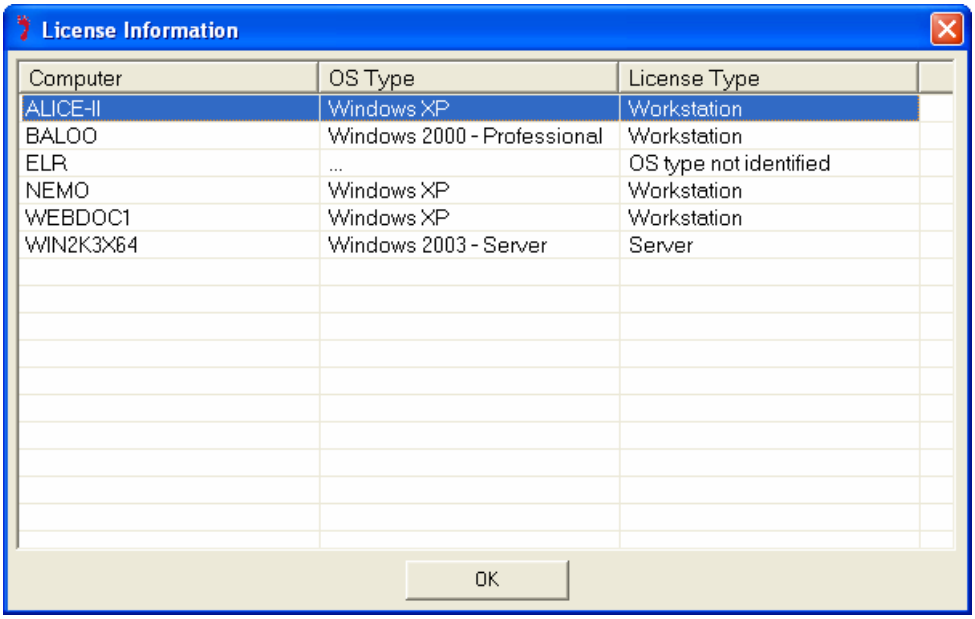
EventTracker displays the Availability of License window.

Figure 13 Availability of License

4 Click **License info**.

EventTracker displays the License Information window.

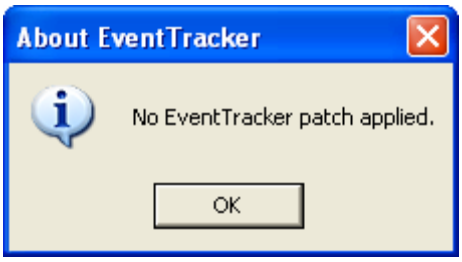
Figure 14 License Information


License Information
Computer OS Type License Type
ALICE-II Windows XP Workstation
BALOO Windows 2000 - Professional Workstation
ELR ... OS type not identified
NEMO Windows XP Workstation
WEBDOC1 Windows XP Workstation
WIN2K3X64 Windows 2003 - Server Server
OK

5 Click **Patch Info** to view the patches applied.

EventTracker displays the patch information.

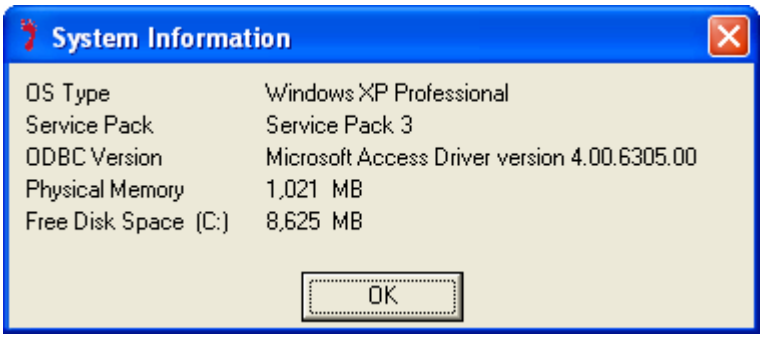
Figure 15 Patch information



6 Click **System Info** to view system information.

EventTracker displays the System Information window.

Figure 16 System Information



EventTracker Components

System Manager

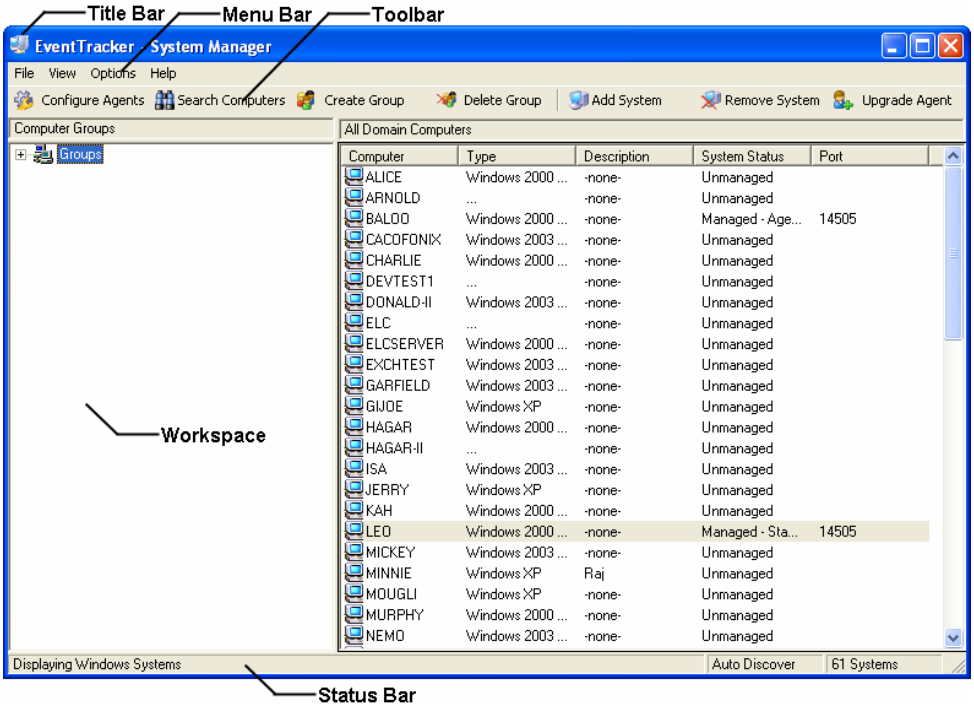
System Manager enables you to manage Computer Groups, Systems, and Agents.

System Manager enables you to:

- Create, Modify, and Delete a Group. You can add systems to the Group by System Type, IP subnet or by manual selection.
- Install, Uninstall, and Upgrade Agents.
- Switch modes of the Agent
- Configure Agents.
- View logs.

To work with EventTracker System Manager effectively, a thorough understanding of its graphical user interface is necessary.

Figure 17 System Manager User Interface



Title Bar

The top strip of System Manager is the Title Bar. Title Bar displays the name of the application. You cannot move or drag the Title Bar.

Menu Bar

The strip next to Title Bar is the Menu Bar. Menu Bar contains menus. Each Menu contains a list of commands and shortcut keys to carry out a specific task. You cannot customize, move, or drag the Menu Bar.

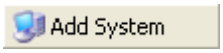
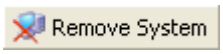
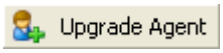
Toolbar

The third strip is the Toolbar. Toolbar contains command buttons with images. Frequently used options are provided on the Toolbar. You cannot customize, move, or drag the Toolbar.

Mouseover ToolTip for command buttons help you know the purpose the buttons serve.

Table 9

Click	To
Configure Agents	Open the Agent Configuration window.
Search Computers	Search and add computers. You can add a single computer or a Group of computes.
Create Group	Create a logical computer Group. You can add systems to the Group by System Type, IP subnet or

Click	To
	manual selection.
	Delete a logical computer Group.
	Install the Agent on remote systems.
	Uninstall the Agent from remote systems.
	Upgrade the Agent. You can upgrade through Windows Domain Network or Upgrade Over IP (Non Windows domain) methods.

Workspace

The workspace consists of a left pane and a right pane.

Left pane displays the tree view of computer Groups.

The right pane displays managed and unmanaged computer details.

Status Bar

System Manager displays the system type i.e. Windows or non-Windows on the left pane, discover mode of System Manager i.e. Auto or Manual in the second section and the total number of systems discovered in the third section on the right pane.

EventVault Warehouse Manager

EventVault Warehouse Manager provides the capability to archive the events from the EventTracker database. The EventVault provides a simple, but important mechanism to securely archive event logs for future use and more specifically for auditing purposes.

In most enterprise networks with multiple critical servers and workstations, the event log data can become huge and unmanageable. Those event data may not be immediately required once the initial analysis is completed. At the same time they cannot be completely discarded, as they will be required for future audits. EventVault solves this problem and provides mechanisms to identify if any of the EventVault data has been tampered with.

Archives are .mdb files that are compressed into .cab files called as "EventBox" and are stored in the Archives folder. If EventTracker is installed in the default path then these files could be located in the Archives directory. The range of events that each EventBox contains is stored into an index file in the archives folder. These EventBoxes are sorted by period and can be viewed from EventVault Manager Window. You can also sort by Name, Checksum, Path, and Port Number.

Figure 18 EventVault Warehouse Manager

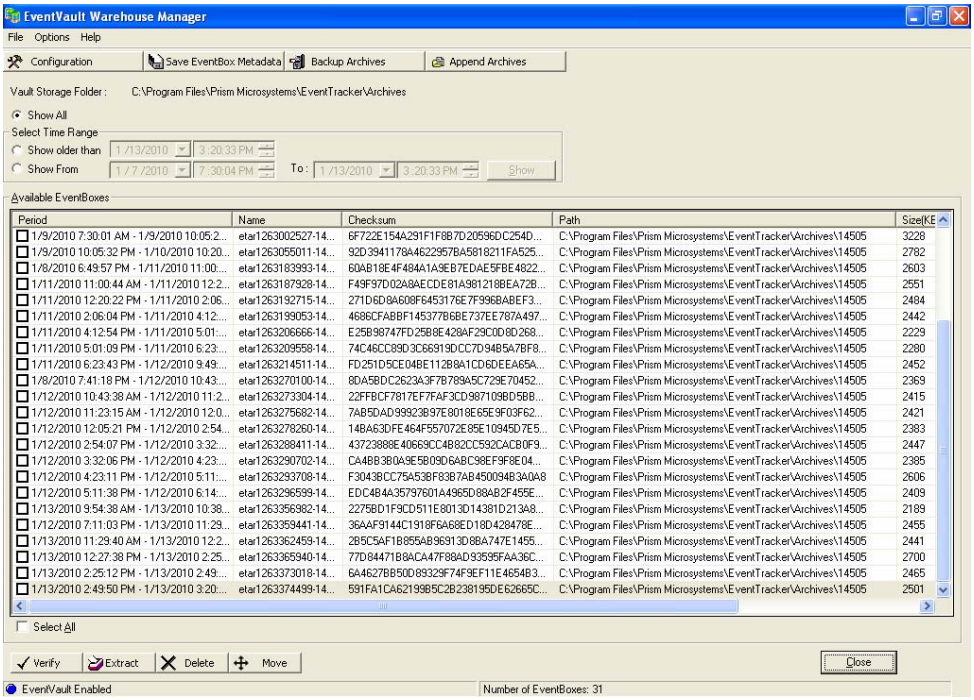


Table 10

Click	To
Configuration	Configure EventVault Warehouse Manager to archive the events from EventTracker database.
Save EventBox Metadata	Save the archive summary into a text file.
Backup Archives	Back up EventVault data for a long-term storage. It helps you to retrieve the backup data if the archives are tampered.
Append Archives	Append CAB files.
Verify	Verify the integrity of selected EventBoxes.
Extract	Extract the selected EventBox data into an MS Access database.
Delete	Delete the selected EventBox.
Show	View the CAB files for a specific period.
Move	Move archives to a new location.

Events Knowledge Base

This option enables you to view event details and Knowledge Base Web site.

To view event details

1. Select an event in the content area.
2. Click the **View** menu and select the **Event Details** option.

   (OR)

   Right-click the event and select the **Event Detail** option from the displayed shortcut menu.

   (OR)

   Double-click the event.

   EventTracker displays the Event Details window.

   EventTracker displays the details for the selected event in the **Event Details** tab.
3. Click **Next>** to view the next event details.
4. Click **<Previous** to view the previous event details.
5. Click the **Knowledge Base** tab.

   EventTracker displays the Knowledge Base tab.
6. Click the hyperlink under **More Information:**

   EventTracker displays the Knowledge Base (http://kb.prismmicrosys.com/) Web site.

EventTracker Diagnostic & Support Tool

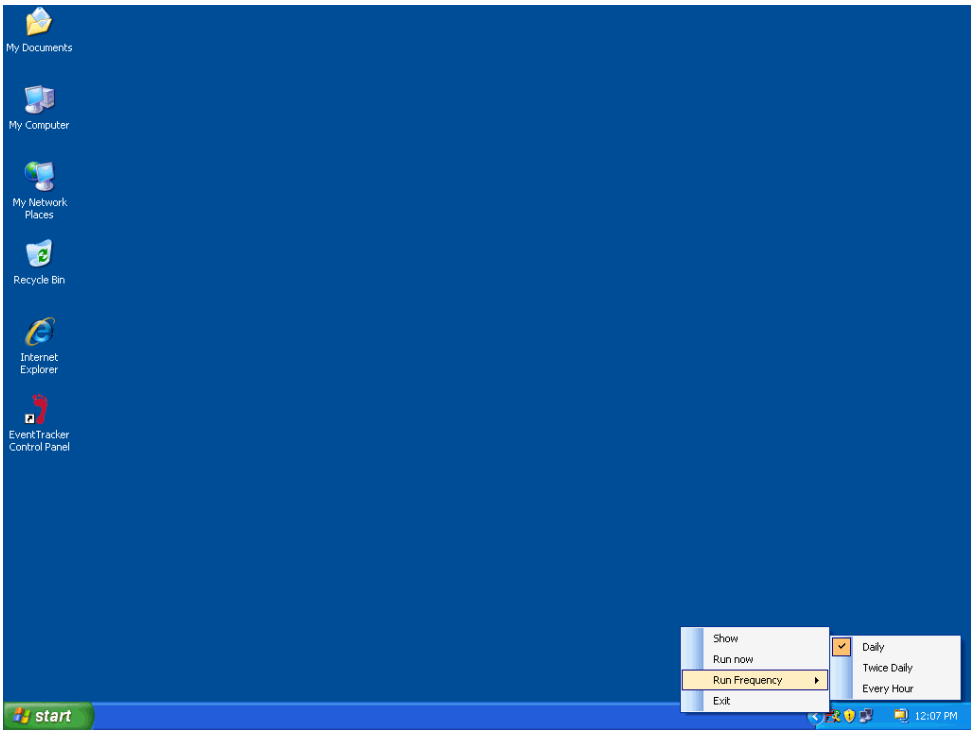
Windows adds the Diagnostic & Support Tool as a Startup program after successful installation of EventTracker.

Figure 19 Diagnostic & Support Tool

Right-click the Diagnostic & Support Tool icon on the taskbar, EventTracker displays the shortcut menu.

To set the frequency, move the mouse pointer over the **Run Frequency** option. EventTracker displays the options to set the frequency.

Figure 20 Diagnostic & Support Tool



Chapter 2
EventTracker Management Console

In this chapter, you will learn how to:

- Choose Columns
- Filter Events from the View
- Filter Events with Exception
- Clear All Events from View
- Reload the Navigation Pane
- Set Auto Scroll option
- Rename a Window

Choosing Columns

This option enables you to select the columns that you want to display on the Dashboard. By default, EventTracker displays Date, Computer, Source, and Description columns on the Dashboard.

To choose columns

1. Click the **Configure** menu and select the **Choose Columns** option.

   EventTracker displays the Choose Columns dialog box.

2. Select the columns and then click **OK**.

> **Note**
>
> To select all the columns, press **+** holding **Ctrl** key on your keyboard.

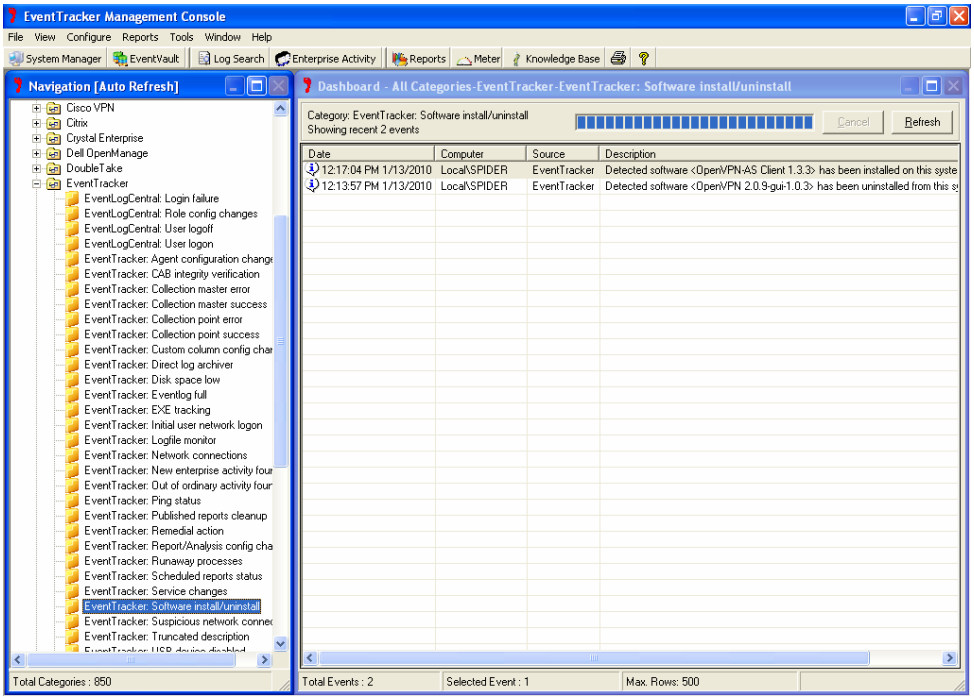
Search Based Console

Search based console helps to search & view events occurred in a specific Category. By default, EventTracker displays number of events as configured in the Manager Configuration window (**Max events view limit (Console)**). Whenever you open the Management Console, EventTracker sets the focus on Correlated Alerts and Incidents Category and displays the events associated with that Category. If there are no events occurred in that particular time frame, EventTracker gives you options to search farther back. You can also configure EventTracker to show/store only the active Alerts through the options provided in the Manager Configuration window.

1. Select an event Category. Example: EventTracker -> EventTracker: Software install/uninstall. You can also select a system and then click an event Category to view events occurred in that Category for that particular system.

   EventTracker displays the events occurred in the selected Category alone in the Dashboard pane.

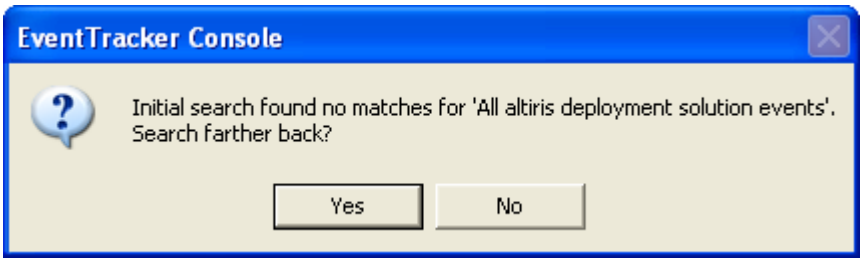
Figure 21 Management Console



2 Click **Refresh** to view recent events.

If initial search is returned with no matching records, then EventTracker displays the EventTracker Console message box.

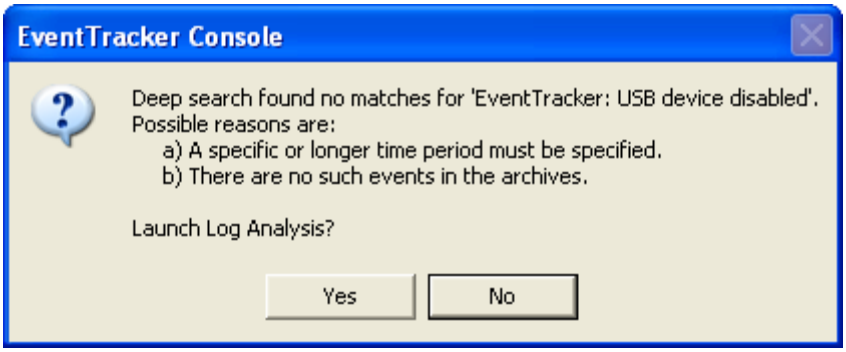
Figure 22 EventTracker Console message box



3 Click **Yes** to continue.

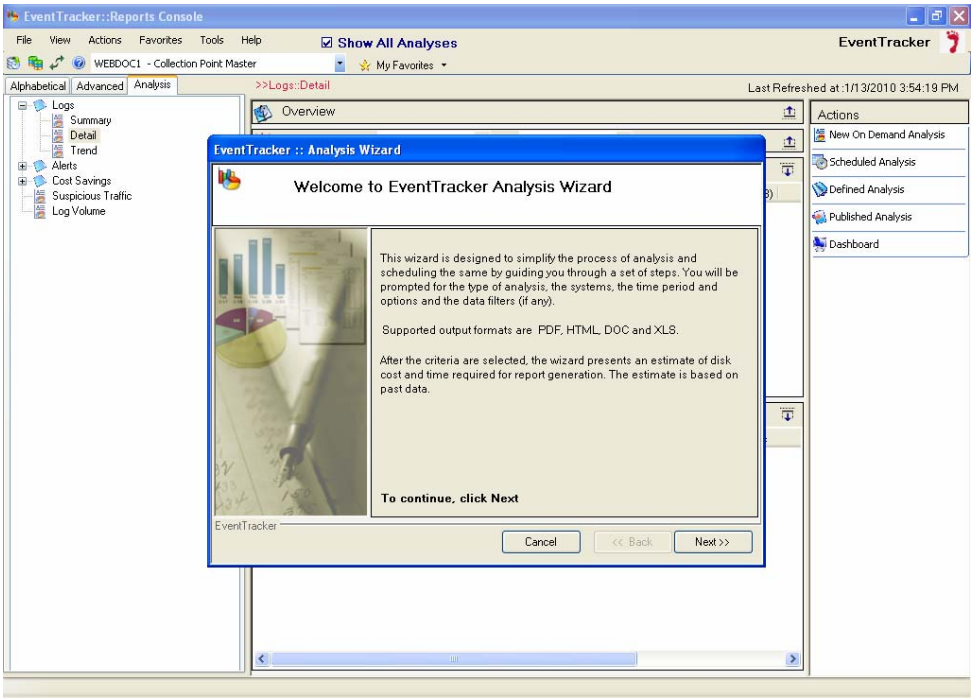
If EventTracker does not find any events, then displays the EventTracker Console dialog box with appropriate message.

Figure 23
EventTracker Console message box


EventTracker Console
Deep search found no matches for 'EventTracker: USB device disabled'.
Possible reasons are:
a) A specific or longer time period must be specified.
b) There are no such events in the archives.
Launch Log Analysis?
Yes
No

4 Click **Yes** to launch Log Analysis.

Figure 24 Reports Console – Log Analysis


EventTracker::Reports Console
File View Actions Favorites Tools Help
Show All Analyses
EventTracker
WEBDOC1 - Collection Point Master
My Favorites
Alphabetical Advanced Analysis
>>Logs::Detail
Last Refreshed at :1/13/2010 3:54:19 PM
Logs
Summary
Detail
Trend
Alerts
Cost Savings
Suspicious Traffic
Log Volume
Overview
Actions
New On Demand Analysis
Scheduled Analysis
Defined Analysis
Published Analysis
Dashboard
EventTracker :: Analysis Wizard
Welcome to EventTracker Analysis Wizard
This wizard is designed to simplify the process of analysis and scheduling the same by guiding you through a set of steps. You will be prompted for the type of analysis, the systems, the time period and options and the data filters (if any).
Supported output formats are PDF, HTML, DOC and XLS.
After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.
To continue, click Next
EventTracker
Cancel
<< Back
Next >>

Filtering Events from View

Fine grain filtering for meaningful monitoring support for both view and source filters based on wildcard matches of id, type, source, user, event description.

- Filter non-essential events – collect and manage only important events – minimum traffic

- Filter any event(s) for display only (these are still logged into the event database)
- Monitor only specific events – examples
  - Log all events into the database but display only Audit Failure
  - Create a separate monitoring window for Exchange Server events
- Filter any specific category of events – example Monitor all events except information events
- Exclusive filters according to your own criteria – examples
  - Filter all Information events except defined list
  - A few specific events are frequently generated but you wish to exclude these and monitor all other events.
- BOOLEAN operators in filter policy definitions – provides the ability to match multiple strings in fields to create sophisticated filter policy definition.

Configuring Event Filters

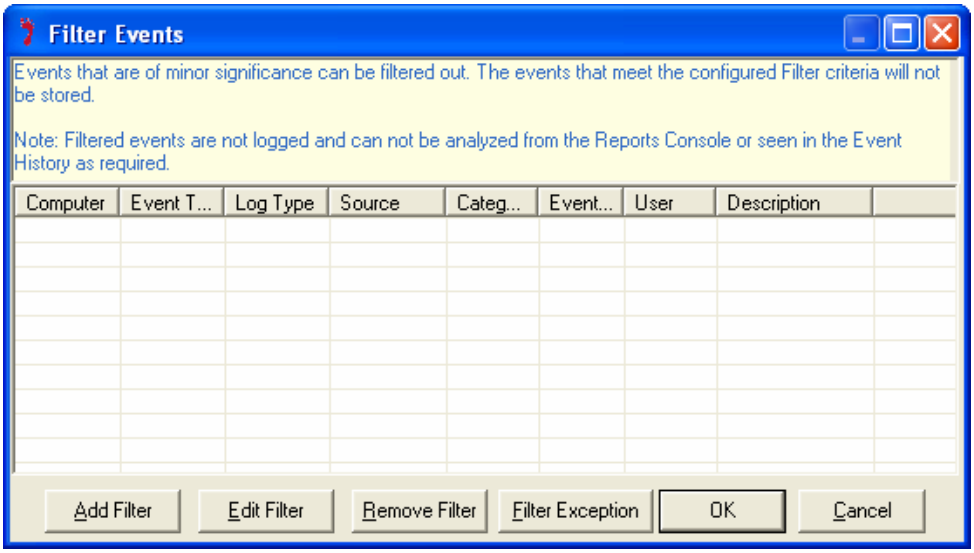
This option enables you to filter events of minor significance from the view. Events are filtered from the view alone and EventTracker keeps logging those events into the database.

To configure event filters

1. Open the Management Console.
2. Click the **Configure** menu and select the **Filter Events** option.

   EventTracker displays the Filter Events console.

Figure 25 Filter Events



3 Click **Add Filter**.

EventTracker displays the Add Event Filter Parameters dialog box.

Figure 26 Add Event Filter Parameters

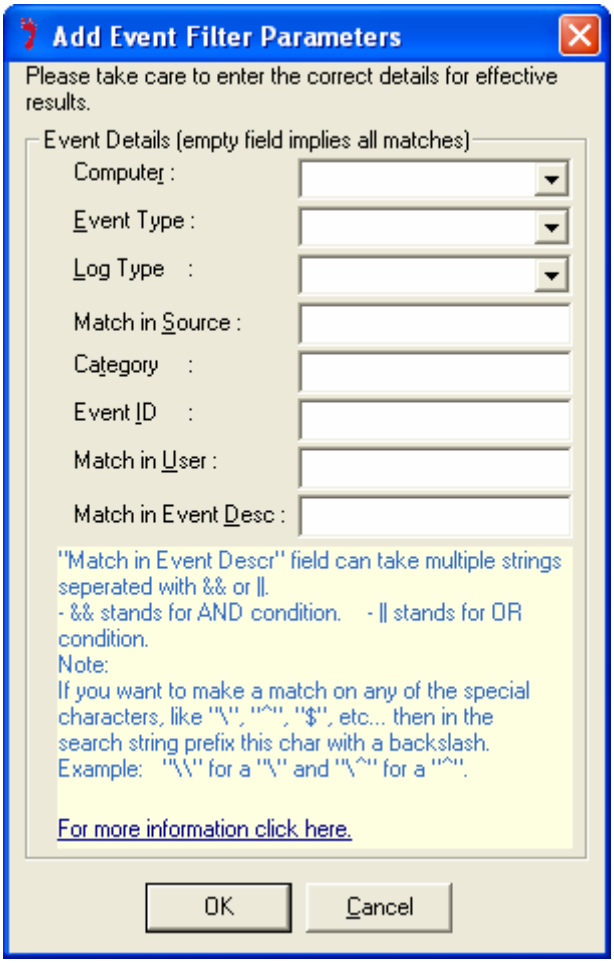

Add Event Filter Parameters
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Computer :
Event Type :
Log Type :
Match in Source :
Category :
Event ID :
Match in User :
Match in Event Desc :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

Table 11

Click	To
Event Details(empty field implies all matches)	
Computer	Select a computer from the drop-down list for which you want to filter out events from view.
Event Type	Classification of event severity: **Error**, **Information**, **Warning** in the System and Application logs; **Success Audit** or **Failure Audit** in the Security log. Select an event type from the drop-down list.
Log Type	Select a log type from the drop-down list.
Match in Source	The software that logged the event, which can be either a program name such as "SQL Server," or a component of the system or of a large program such as a driver name. For example, "Elnkii" indicates an EtherLink II driver. Type the source in this field.

Click	To
Category	Classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in Group Policy. Type the category number in this field. This field supports numeric data type only.
Event ID	A number identifying a particular event. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems. Type the event ID number in this field. This field supports numeric data type only.
Match in Event Descr.	Type a sub-string of the description that needs to be matched. EventTracker supports multiple strings separated by the following operands. **&&** stands for **AND** condition. **II** stands for **OR** condition. If you type Successful Logon && New Trusted Domain II Removing Trusted Domain, EventTracker will filter out the events that are matching Successful Logon, (AND) New Trusted Domain (OR) Removing Trusted Domain.

Table 12

Event Type	Description
Error	A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error will be logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning will be logged.
Information	In event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.
Audit Success	An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.
Audit Failure	An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

Table 13

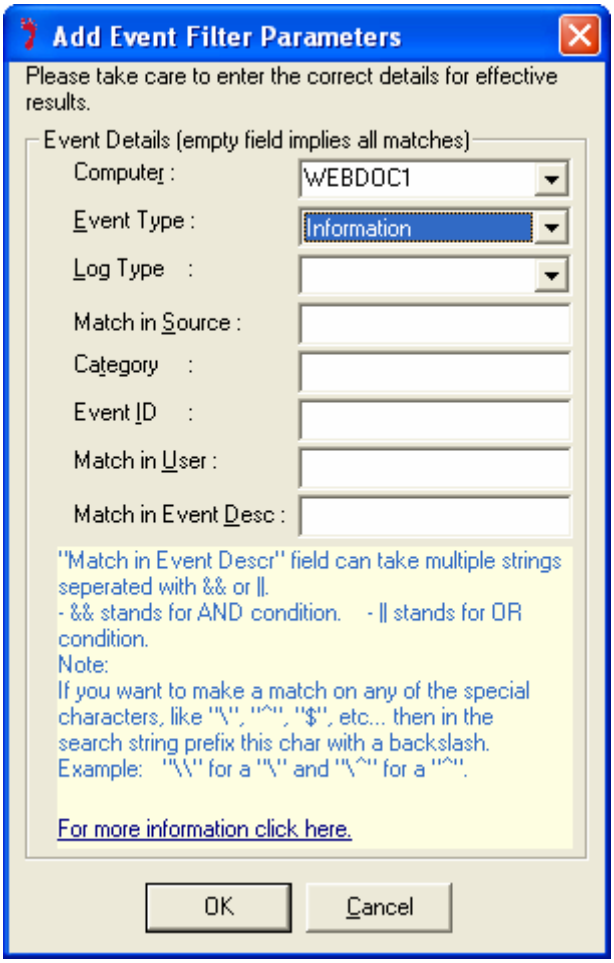
Event log	Log file	Function	Availability
Application log	AppEvent.evt	Records events as determined by each software vendor	All Windows systems
Security log	SecEvent.evt	Records events based on how audit policy is configured	All Windows systems
System log	SysEvent.evt	Records events for Windows operating system components	All Windows systems
Directory Service log	NTDS.evt	Records events for Active Directory	Domain controllers only
DNS Server log	DnsEvent.evt	Records events for DNS servers and name resolution	DNS servers only
File Replication Service log	NtFrs.evt	Records events for domain controller replication	Domain controllers only

Note

If you leave a field blank, EventTracker assumes a wildcard match for that field. For example, leaving the user field blank implies that any value in that field is acceptable.

4 Type appropriately in the relevant fields.

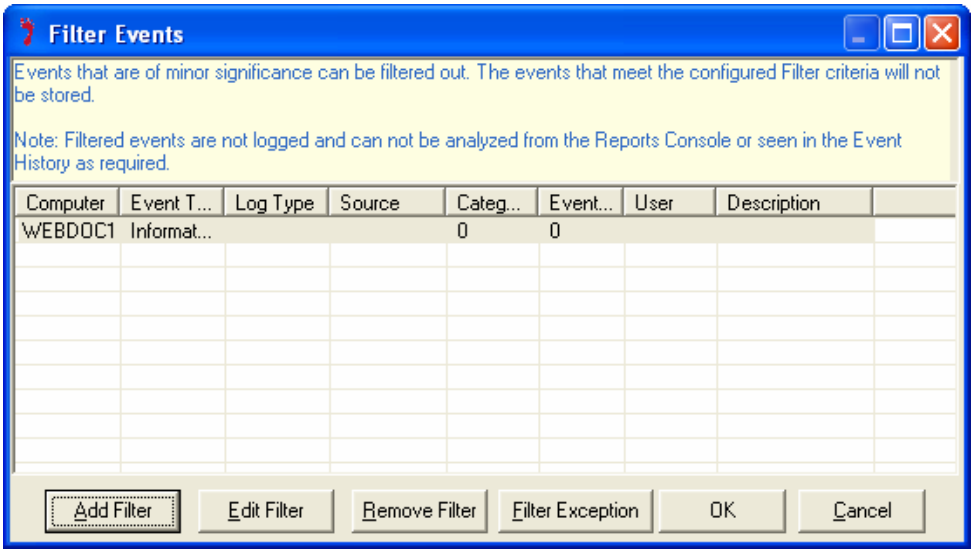
Figure 27 Add Event Filter Parameters


Add Event Filter Parameters
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Computer :
WEBDOC1
Event Type :
Information
Log Type :
Match in Source :
Category :
Event ID :
Match in User :
Match in Event Desc :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

5 Click **OK**.

EventTracker displays the Filter Events console with newly added filter.

Figure 28 Filter Events



6 Click **OK**.

7 Restart the Management Console.

Modifying Event Filter settings

This option enables you to modify filter events configuration settings.

To modify event filter configuration settings

1 Open the **Filter Events** console.

EventTracker displays the Filter Events console.

2 Select the filter from the list and then click **Edit Filter**.

EventTracker displays the Add Event Filter Parameters dialog box.

For field descriptions, refer to Figure 37 Add Event Filter Parameters on page 46.

3 Enter/select appropriately in the relevant fields.

4 Click **OK**.

EventTracker displays the Filter Events console with the modified filter.

5 Click **OK**.

6 Restart the Management Console.

Deleting Event Filters

This option enables you to delete the event filters.

To delete event filters

1. Open the **Filter Events** console.

   EventTracker displays the Filter Events console.

2. Select the filter information that you want to delete in the list.
3. Click **Remove Filter**.

   EventTracker displays the EventTracker Console confirmation message box.

4. Click **Yes**.

   EventTracker deletes the selected filter.

Configuring Event Filters with Exception

This option enables you to filter events with exception. Suppose, you want to filer out all Information Event Type events but interested in monitoring a particular event. You can do this with the Filter Exception option in the Filter Events console.

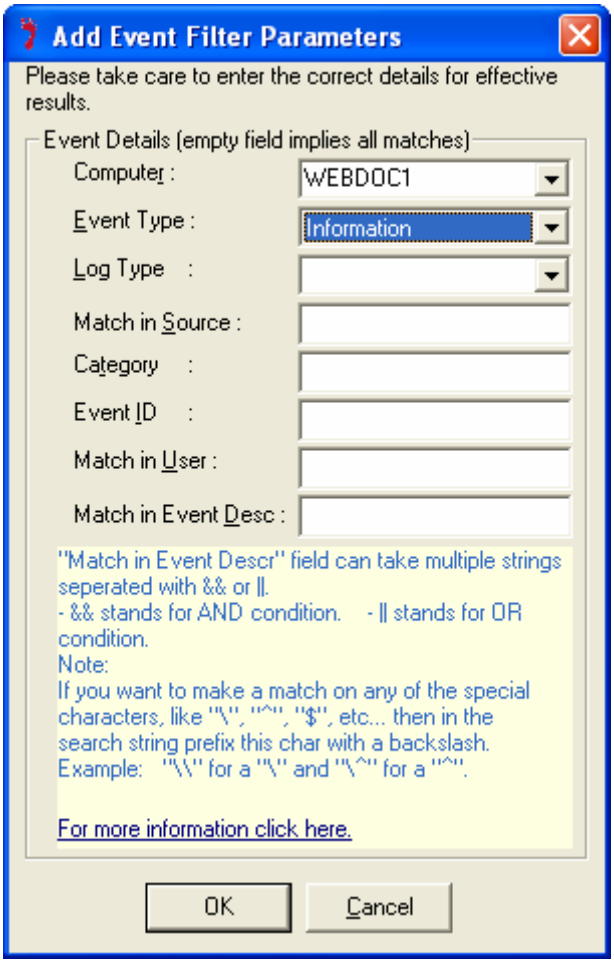
To configure event filters with exception

1. Open the **Filter Events** console.
2. Click **Add Filter**.

   EventTracker displays the Add Event Filter Parameters dialog box.

3. Enter/select appropriately in the relevant fields.

Figure 29 Add Event Filter Parameters


Add Event Filter Parameters
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Computer :
WEBDOC1
Event Type :
Information
Log Type :
Match in Source :
Category :
Event ID :
Match in User :
Match in Event Desc :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

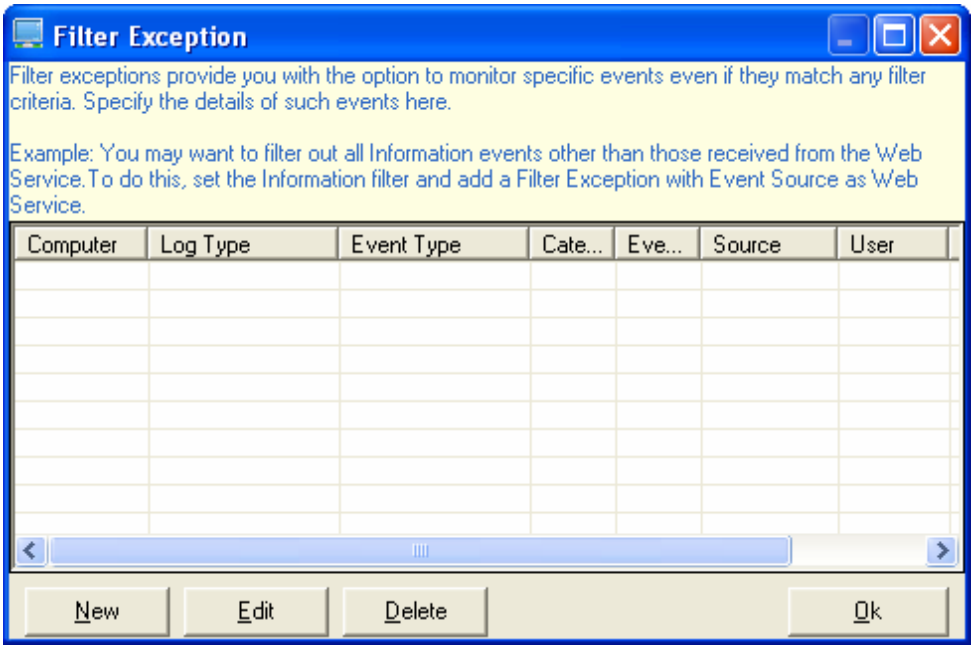
4 Click **OK**.

EventTracker displays the Filter Events console with the newly added filter.

5 Click **Filter Exception**.

EventTracker displays the Filter Exception console.

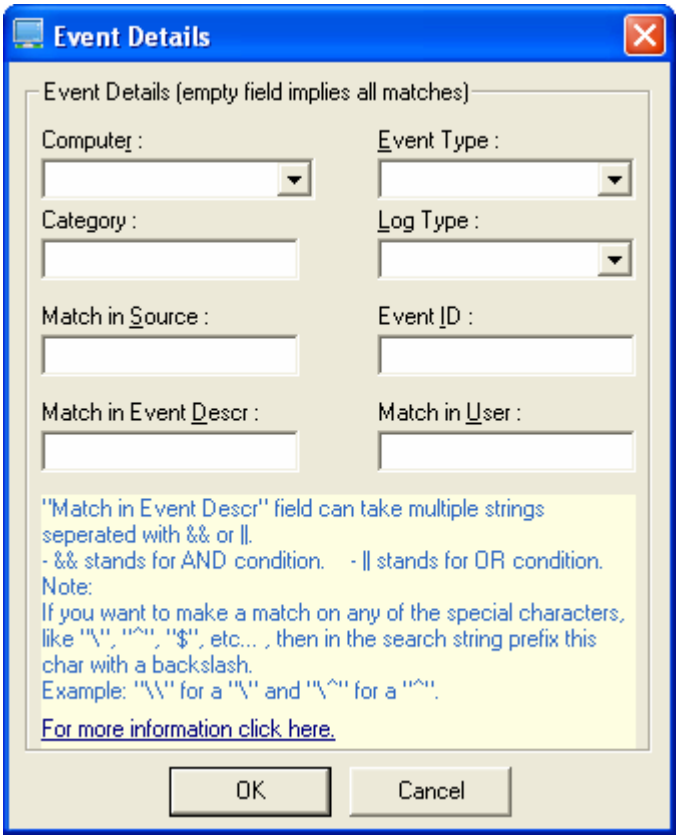
Figure 30 Filter Exception


Filter Exception
Filter exceptions provide you with the option to monitor specific events even if they match any filter criteria. Specify the details of such events here.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.
Computer
Log Type
Event Type
Cate...
Eve...
Source
User
New
Edit
Delete
Ok

6 Click **New** to add new filter exception criteria.

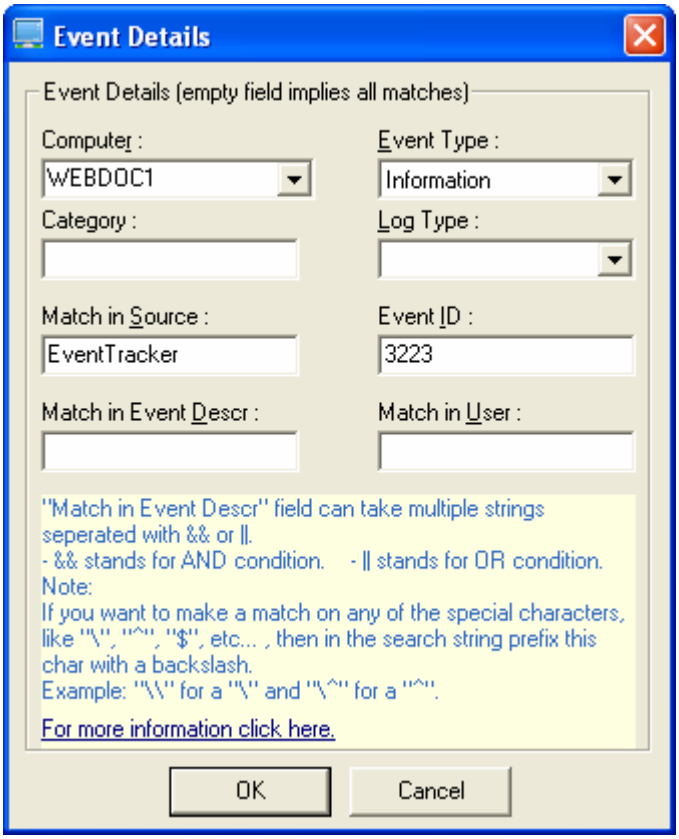
EventTracker displays the Event Details console.

Figure 31 Event Details


Event Details
Event Details (empty field implies all matches)
Computer :
Event Type :
Category :
Log Type :
Match in Source :
Event ID :
Match in Event Descr :
Match in User :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

7 Enter/select appropriately in the relevant fields.

Figure 32 Event Details


Event Details
Event Details (empty field implies all matches)
Computer :
WEBDOC1
Event Type :
Information
Category :
Log Type :
Match in Source :
EventTracker
Event ID :
3223
Match in Event Descr :
Match in User :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

8 Click **OK**.

EventTracker displays the Filter Exception console with newly added filter exception.

9 Click **OK**.

10 Click **OK** on the Filter Events console.

11 Restart the Management Console.

Note

In the above scenario, all events of Information Event Type will be filtered out but with one exception of event **3223**.

Understanding Filters and Filter Exceptions

This section helps you understand how filters and filter exceptions work.

To understand Filters and Filter Exceptions

1. Open the **Filter Events** console.
2. Select the Filter and then click **Remove Filter**.

   EventTracker displays the EventTracker Console message box.
3. Click **Yes**.

   EventTracker removes the selected filter.
4. Click **Filter Exception**.

   The filter exception you have set earlier remains unaltered.
5. Select the filter exceptions and then click **Delete**.

   EventTracker displays the EventTracker Console message box.
6. Click **Yes**.

   EventTracker removes the selected filter exception.

Note

So it is obvious from the above scenario, it is your responsibility to manage Filters and Filter Exceptions. The table given below will provide you a vivid idea how the combination of Filters and Filter Exceptions work.

Table 14

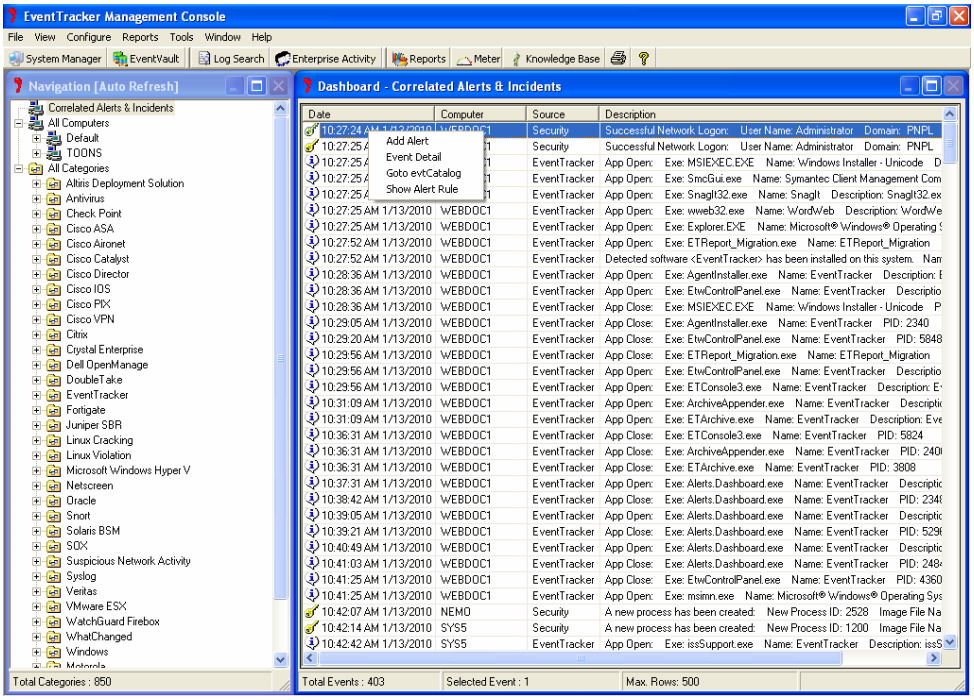
Filter	Filter Exception	Result
Y	**N**	EventTracker filters all events from the view.
N	**Y**	EventTracker allows all events.
Y	**Y**	EventTracker allows events with exception.
N	**N**	EventTracker allows all events.

Viewing and Editing Alert Details

This option facilitates to locate alert from the alert event displayed in the Management Console.

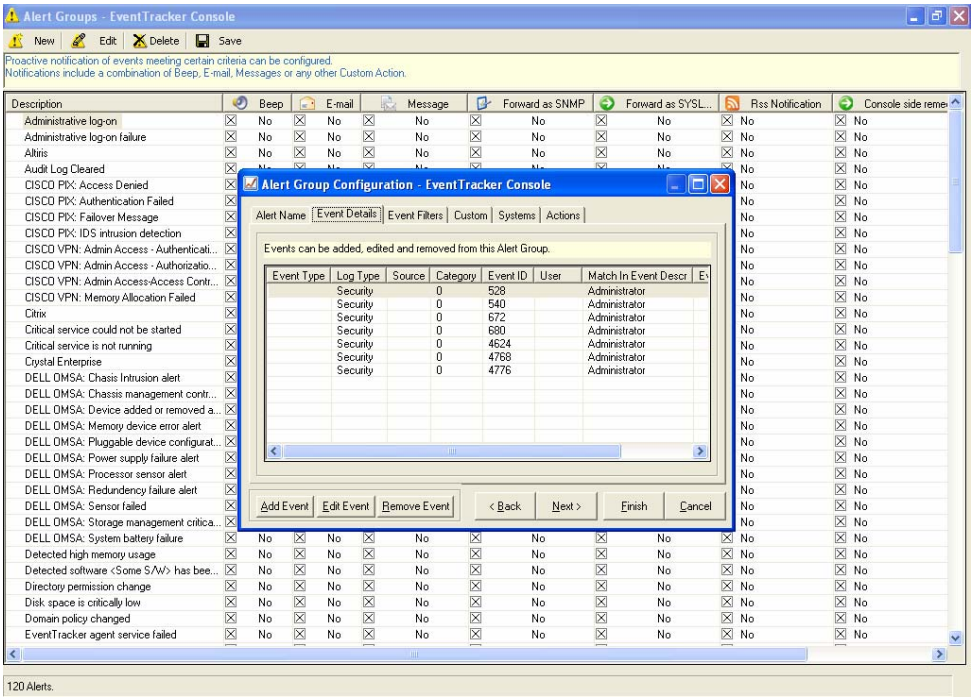
- Right-click an event and select the **Show Alert Rule** option from the shortcut menu to view the exact alert, which caused this event.

Figure 33 Management Console



EventTracker opens the Alert Groups console and focuses on the Alert that caused this event. Also, opens the Alert Group Configuration window and displays the Event Details.

Figure 34 Alert Groups



Reloading the Navigation Pane

Press F5 to refresh the Categories and Systems. Pressing Ctrl + F5 to reload and refresh the Navigation Pane with the changes made in the System Manager.

This option enables you to reload the Navigation Pane

To add a new Group, reload and refresh the Navigation pane

1. Open the Management Console.

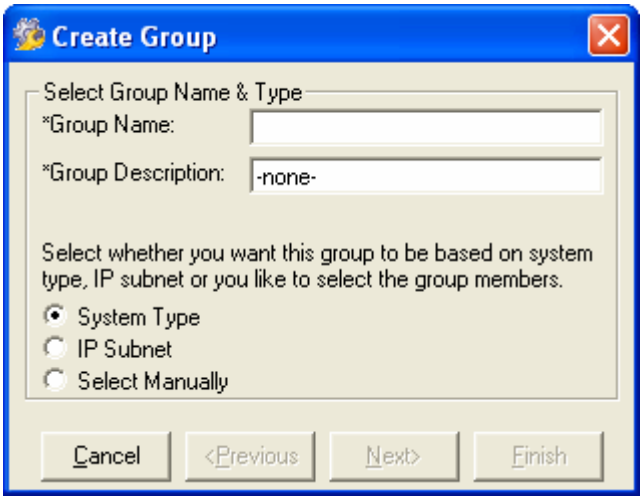
   EventTracker displays the Navigation pane with the existing Group(s).

2. Open the System Manager.

3. Click **Create Group** on the toolbar.

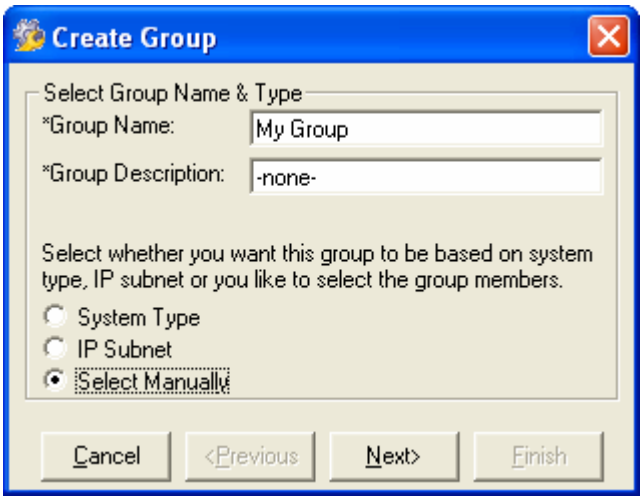
   EventTracker displays the Create Group dialog box.

Figure 35 Create Group



4 Type the **Group Name** and **Description** and then select the option to add members to your Group.

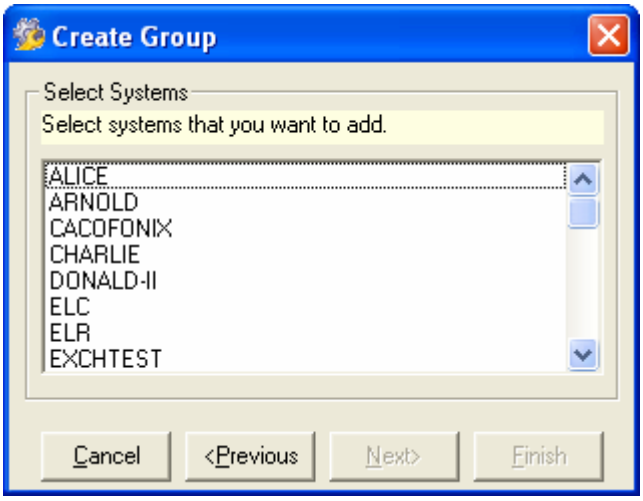
Figure 36 Create Group



5 Click **Next>**.

EventTracker displays the systems available for selection.

Figure 37 Create Group

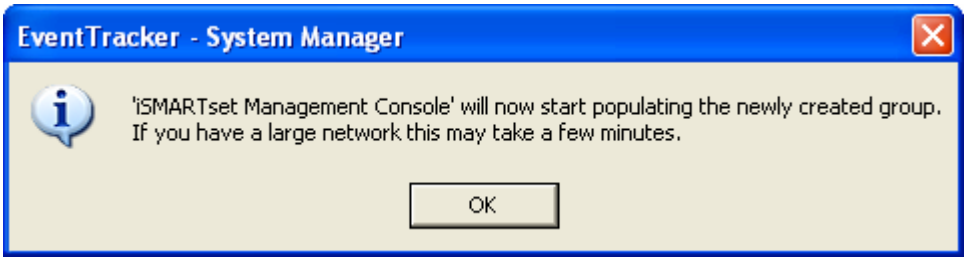


6 Select the Systems.

7 Click **Finish**.

EventTracker displays the System Manager message box.

Figure 38 System Manager message box


EventTracker - System Manager
'iSMARTset Management Console' will now start populating the newly created group.
If you have a large network this may take a few minutes.
OK

8 Click **OK**.

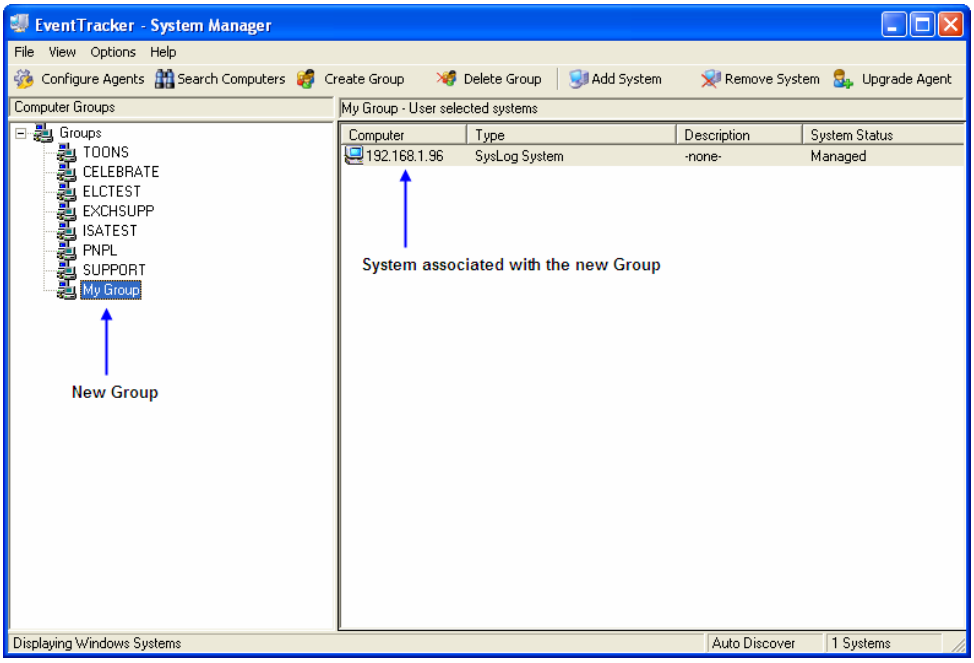
EventTracker displays the System Manager message box after populating your Group.

Figure 39 System Manager message box

9 Click **OK**.

EventTracker displays the System Manager with the newly created Group.

Figure 40
EventTracker - System Manager



Although, the Management Console is in Auto Refresh mode, the Navigation pane is not updated with the new Group.

10 Click the **View** menu and select the **Refresh Systems** option or press **Ctrl + F5** on the keyboard.

EventTracker refreshes the Navigation pane by fetching the latest data from the database.

Auto Scrolling Option

Enabling the auto-scroll option will cause the Events window on the Management Console to automatically scroll down (and select) the latest event. By default, EventTracker enables this option.

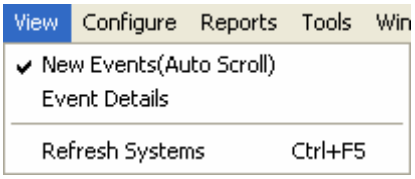
To select the latest event automatically

- Click the **View** menu and select the **New Events (Auto Scroll)** option.

  A tick mark appears before the New Events (Auto Scroll) option.

  Clear the tick mark to disable this option.

Figure 41 Auto Scroll



Printing Current View Event details

This option enables you to print current view event details.

To print current view event details

1. Open the Management Console.
2. Select the System or the Category in the Navigation pane. Example: System – WEBDOC1.
3. Click on the toolbar.

   (OR)

   Click the **File** menu and select the **Print** option

   (OR)

   Press **Ctrl+P** on your keyboard.

   EventTracker displays the report.

Chapter 3
Configuring Manager

In this chapter, you will learn how to:

- Set Window View Limit (Console)
- Configure EventTracker Knowledge Base Web site
- Monitor Agent Health
- Configure SYSLOG Receiver
- Monitor Syslogs
- Configure Virtual Collection Points for Syslogs
- Configure EventTracker Receiver Ports
- Forward Raw Syslog messages
- Configure Virtual Collection Points
- Configure Correlation Receiver
- Configure Direct Log File Archiver
- Enable Alert Notification Status Tracking
- Purge Alert Events Cache
- Configure Manager to show only active Alert events in Console
- Configure Manager to store only active Alert events
- Enable Remedial Actions
- Suppress Duplicate Alerts
- Configure Manager to Alert Suspicious Network Activity

Setting the Window View Limit (Console)

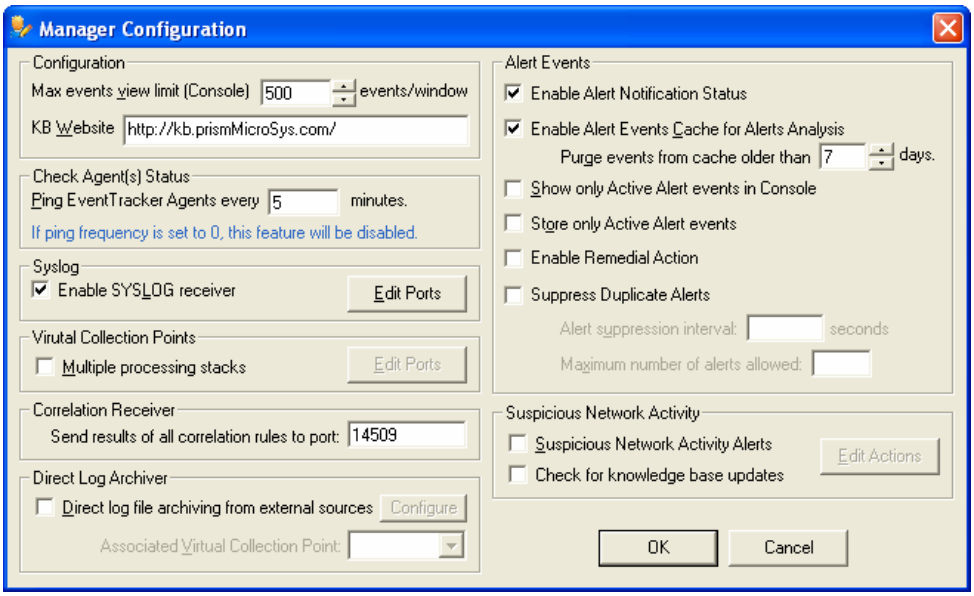
This option enables you to set the Management Console Dashboard view limit.

To set the Dashboard view limit

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.

Figure 42 Manager Configuration



3. Type or select the number of events that you want to display in the Dashboard from the **Max events view limit (Console)** spin box.
4. Click **OK**.

   EventTracker displays the confirmation message box.
5. Click **Yes** to save the changes.

EventTracker Knowledge Base Web site

This option enables you to configure EventTracker Knowledge Base Web site.

To configure EventTracker knowledge Base Web site

1. Open the Management Console.

2 Click the **Configure** menu and select the **Configure Manager** option.

EventTracker displays the Manager Configuration window.

3 Type the URL of the Knowledge Base Web site in the **KB Website** field.

4 Click **OK**.

EventTracker displays the confirmation message box.

5 Click **Yes** to save the changes.

SYSLOG Receiver

EventTracker selects the Enable Syslog Receiver check box by default to enable the EventTracker Receiver to receive SYSLOGs sent by non-Windows systems.

To disable SYSLOG receiver

1 Open the Management Console.

2 Click the **Configure** menu and select the **Configure Manager** option.

EventTracker displays the Manager Configuration window.

Enable SYSLOG receiver check box is selected by default.

3 Clear the check box.

4 Click **OK**.

EventTracker displays the confirmation message box.

5 Click **Yes** to save the changes.

Monitoring Syslogs

For monitoring Syslog events, you must configure the UNIX computer to forward Syslog events to the computer where the EventTracker Manager is installed. The default Syslog port is UDP Port=514. Also see the FAQ on Syslog.

To configure UNIX systems to forward Syslog messages to EventTracker

1 Identify the IP Address of the computer that is hosting the EventTracker Manager.

2 Log on with the root account in the UNIX computer.

3 Open the syslog.conf file in a text editor. The default path of the syslog.conf file is /etc/syslog.conf.

4 Append the configuration details in the syslog.conf file to forward Syslog messages to the EventTracker Manager computer.

5 Save and close the syslog.conf file.

6 Stop and restart the Syslog daemon (syslogd).

Example: To forward syslog error messages to the IP address 192.192.150.150, add the following detail to the syslog.conf file. *.err @192.192.150.150

Note

For more information refer the syslog.conf or syslog MAN pages.

Syslog configuration may be platform-dependent and it is recommended that you check the platform documentation.

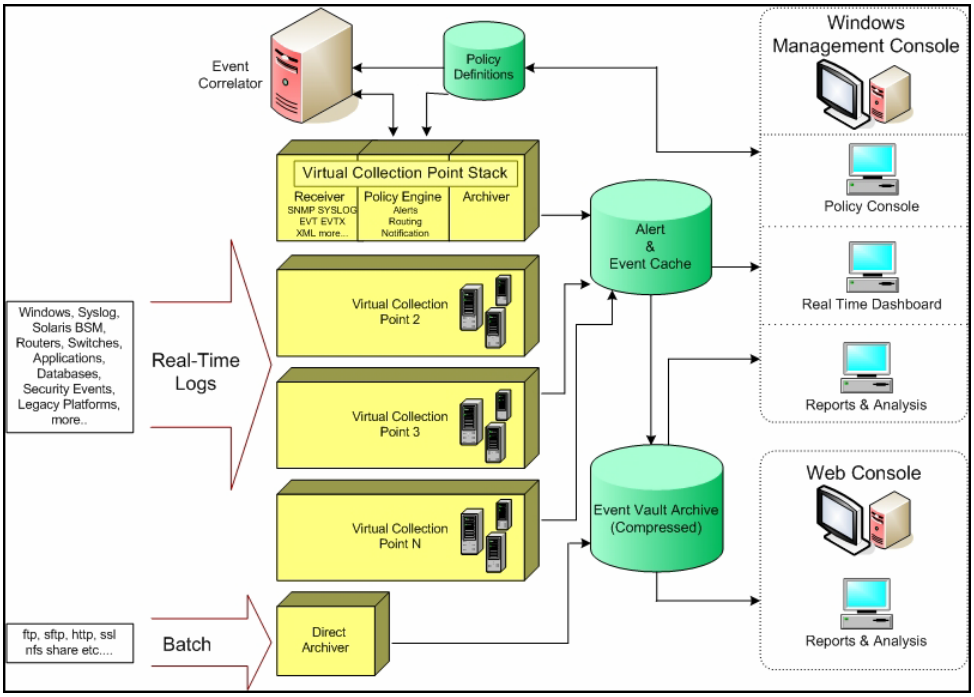
Virtual Collection Points

Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires a number of hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.

VCP Architecture

Figure 43 VCP Architecture



Configuring EventTracker Receiver to listen on multiple ports

EventTracker Receiver can be configured to listen on 10 ports for Traps and 20 (10 UDP & 10 TCP) ports for Unix/Linux/Solaris Syslogs.

Table 15

ET Modules	Suggested Trap Ports
You need to add the ports that you are using to the Firewall exceptions list.	
EventTracker Receiver (Incoming)	14505 default port. 14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585, 14595 (max 10 ports) 514 default UDP for Syslogs. 1470 default TCP for Syslogs. You can add max 10 UDP and 10 TCP ports.
The following ports are internally fixed. You cannot edit these ports. Communication through these ports is taken care internally, which means the number of ports utilized by the respective modules will be in proportion to the number of trap ports set.	
User Activity (Incoming)	14556,14557,14558,14559,14560,14561,14562,14563,14564,14565,14566,14567,14568,14569,14570,14571,14572,14573,1457

ET Modules	Suggested Trap Ports
	4,14575
Correlator (Incoming)	14656,14657,14658,14659,14660,14661,14662,14663,14664,14665,14666,14667,14668,14669,14670,14671,14672,14673,14674,14675
EventTracker Receiver (Outgoing - for viewers)	32001,32002,32003,32004,32005,32006,32007,32008,32009,32010,32011,32012,32013,32014,32015,32016,32017,32018,32019,32020

For more information, refer

http://www.prismmicrosys.com/resources/documents/VCP.pdf

Virtual Collection Points for Syslogs

EventTracker Receiver can be configured to listen on 20 (10 UDP & 10 TCP) ports for Unix/Linux/Solaris Syslogs.

Configuring EventTracker Receiver Ports

This option helps you configure EventTracker Receiver to listen on different ports.

To configure virtual collection points for syslogs

1. **Enable SYSLOG receiver** check box is checked by default. Click **Edit Ports**.

   EventTracker displays the Virtual Collection Points for Syslogs window.

Figure 44 Virtual Collection Points for Syslogs

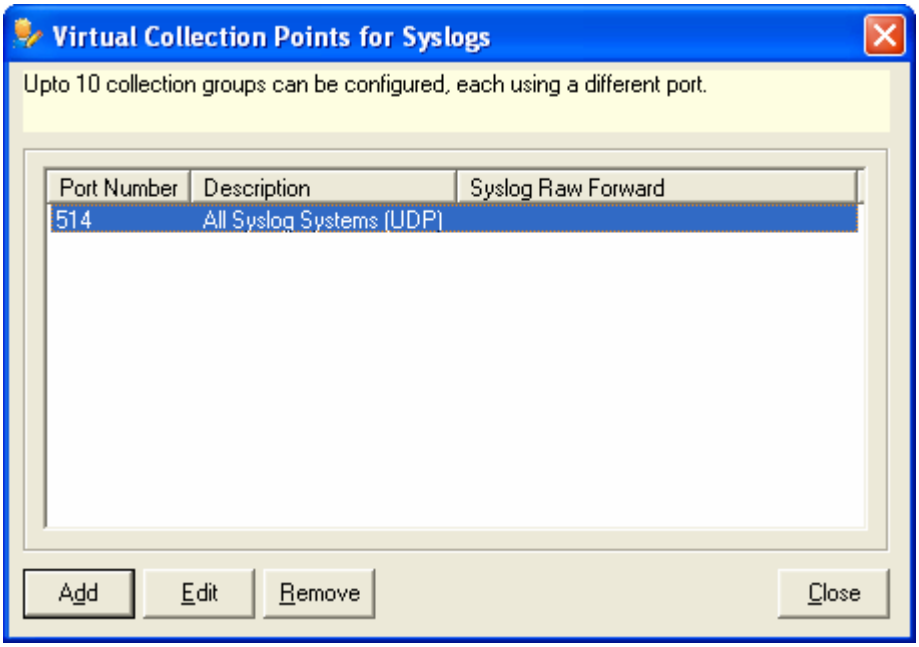


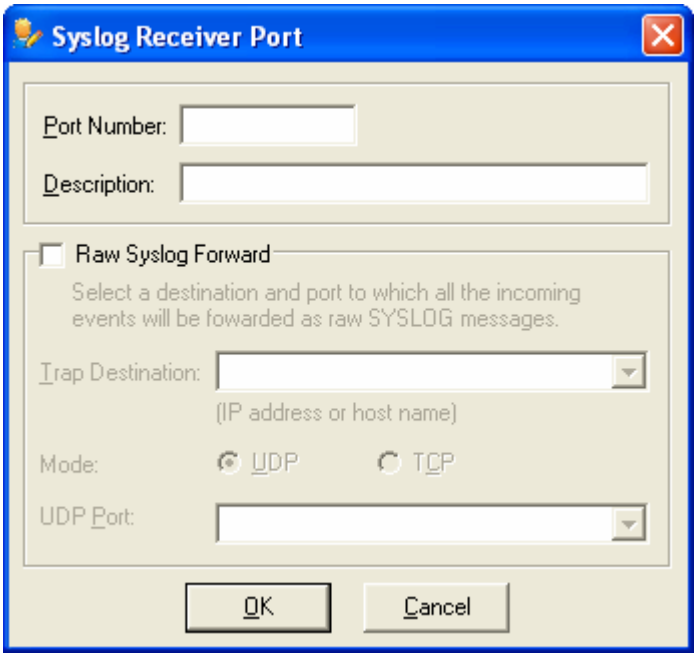
Table 16

Click	To
Add	Add UDP, TCP ports.
Edit	Edit ports.
Remove	Remove ports.

2 Click **Add**.

EventTracker displays the Syslog Receiver Port window.

Figure 45 Syslog Receiver Port



3 Type appropriate port details and then click **OK**.

EventTracker adds the newly configured ports.

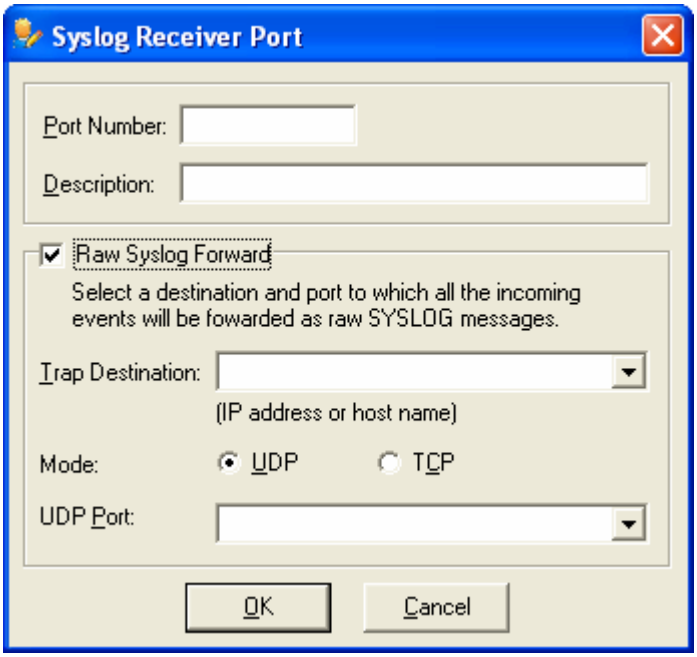
Forwarding Raw Syslog messages

This option helps you forward received Syslog messages in raw format i.e. forwarded with the same format as it is received to a specified destination.

To forward Syslog messages in raw format

1 Select the **Raw Syslog Forward** check box.

Figure 46 Forwarding raw Syslog messages



2. Type the name or IP address of the destination in the **Trap Destination** field.
3. Select an appropriate **Mode** of transport.
4. Select an appropriate port with respect to the mode chosen.
5. Click **OK**.
6. Click **Close**.
7. Click **OK** on the Manager Configuration window.

Virtual Collection Points for Windows Events

EventTracker Receiver can be configured to listen on 10 ports for Windows Events.

Example Scenario

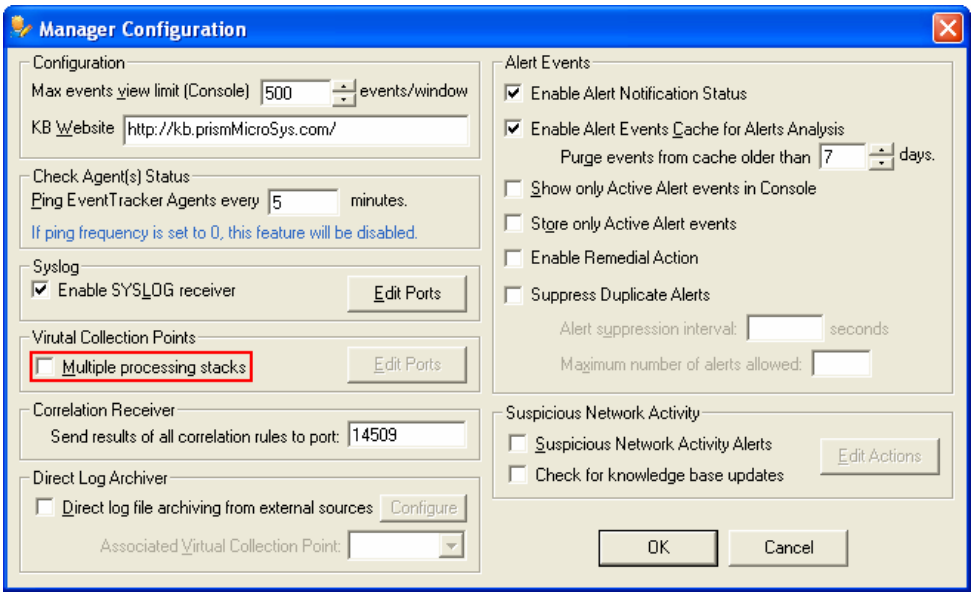
Consider EventTracker Agents in computers Sys2 and Sys3 are forwarding events to Sys1 (EventTracker Manager). By default, the communication happens through port 14505. Suppose you want to configure different ports 14515 and 14525 for Sys2 and Sys3 respectively, do the following:

Computer: Sys1 – Configuring Ports

1. Double-click **Manager Configuration** on the Control Panel.

EventTracker displays the Manager Configuration window.

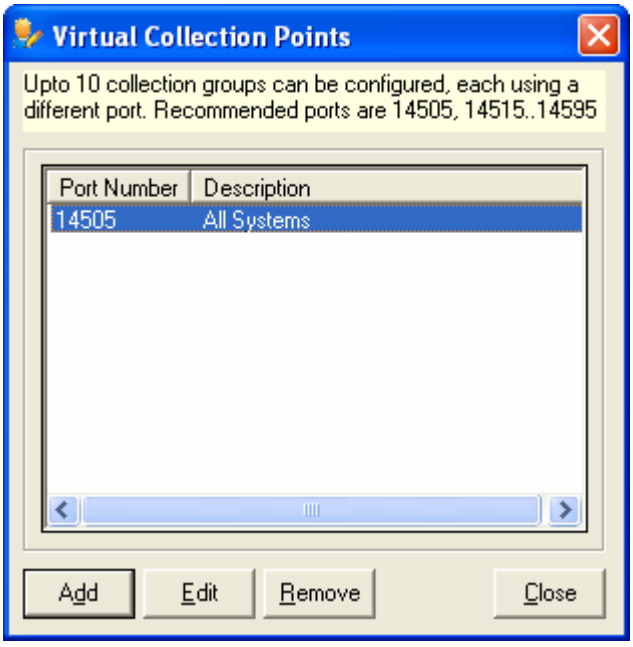
Figure 47 Manager Configuration



2 Select the **Multiple processing stacks** check box.

EventTracker displays the Virtual Collection Points dialog box.

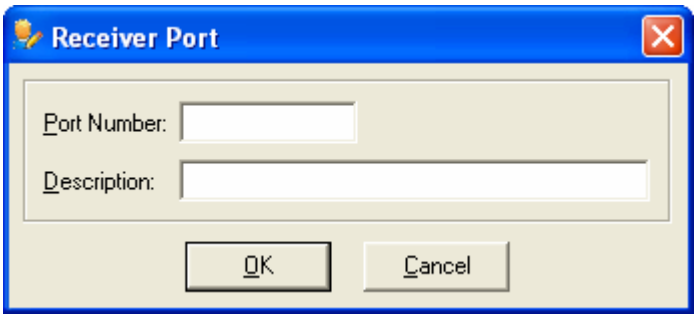
Figure 48 Virtual Collection Points



3 Click **Add**.

EventTracker displays the Receiver Port dialog box.

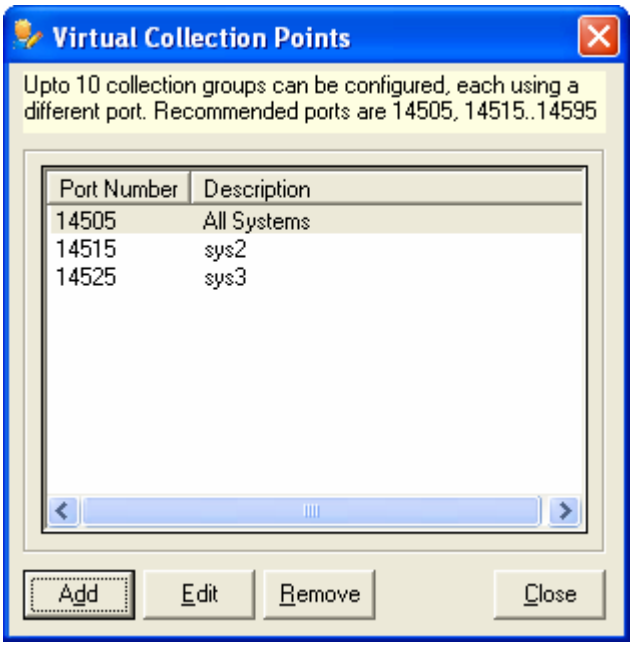
Figure 49 Receiver Port



4 Add Receiver ports and then click **OK**. (Example: 14515, 14525)

EventTracker adds the newly configured ports.

Figure 50 Virtual Collection Points

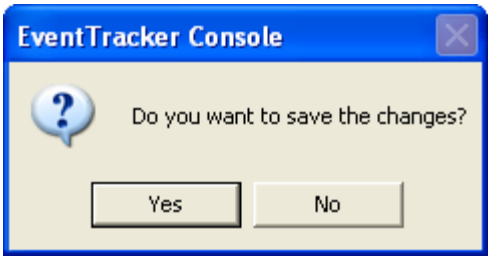


5 Click **Close**.

6 Click **OK** on the Manager Configuration window.

EventTracker displays the EventTracker Console confirmation message box.

Figure 51
EventTracker Console confirmation message box

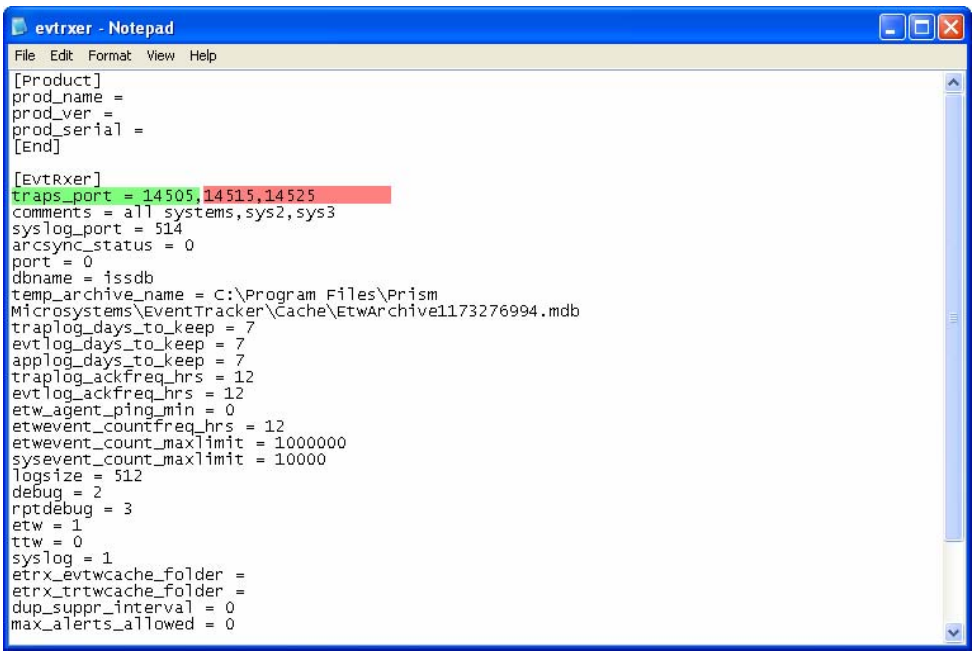


7 Click **Yes** to save the changes.

8 Restart the Management Console.

EventTracker updates these changes in evtrxer.ini file (…\Program Files\Prism Microsystems\EventTracker)

Figure 52 evtrxer.nin file



Note

EventTracker creates ***EtaConfig_14515.ini*** & ***EtaConfig_14525.ini*** files in RemoteInstaller folder (…\Program Files\Prism Microsystems\EventTracker\RemoteInstaller).

9 Restart the EventTracker Receiver service.

Table 17

EventTracker Modules	Trap Ports utilized
You need to add these ports to the Firewall exceptions list.	
EventTracker Receiver (Incoming)	14505, 14515, 14525
User Activity (Incoming)	14556, 14557, 14558
Correlator (Incoming)	14656, 14657, 14658
EventTracker Receiver (Outgoing - for viewers)	32001, 32002, 32003

Upgrading Agent (Sys2) from Manager (Sys1)

1. Open the System Manager console.
2. Click **Upgrade Agent** on the toolbar.
3. Select and Add> Sys2 to Selected Computers list.
4. Select an appropriate **Upgrade Method**.
5. Click **Advanced**.
6. Select **Custom Config** option.
7. Click **Browse** and locate EtaConfig_14515.ini file in the RemoteInstaller folder.
8. Click **Upgrade**.

   EventTracker overwrites etaconfig.ini file with new settings.

Upgrading Agent (Sys3) from Manager (Sys1)

1. Open the System Manager console.
2. Click **Upgrade Agent** on the toolbar.
3. Select and Add> Sys3 to Selected Computers list.
4. Select an appropriate **Upgrade Method**.
5. Click **Advanced**.
6. Select **Custom Config** option.

7. Click **Browse** and locate EtaConfig_14525.ini file in the RemoteInstaller folder.
8. Click **Upgrade**.

   EventTracker overwrites etaconfig.ini file with new settings.

Configuring Correlation Receiver

This option helps you configure correlation receiver port to receive results of correlation rules.

To configure correlation receiver port

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   By default, correlation receiver receives rules through port **14509**.
3. Type the port number in the **Send results of all correlation rules to port** field.
4. Click **OK**.
5. Click **Yes** to save the changes.

Direct Log File Archiving

This option helps you archive log files collected from external sources.

To archive log files collected from external sources

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.
3. Select the **Direct log file archiving from external sources** check box.
4. Select a port from the **Associated Virtual Collection Point** drop-down list.

   Assign an exclusive port that is not associated with any collection groups.
5. Click **OK**.
6. Click **Yes** to save the changes.

   For more information, refer

   http://www.prismmicrosys.com/resources/documents/EventTracker%20v6.3%20Direct%20Log%20Archiver.pdf

Enabling Alert Notification Status Tracking

This option helps you track success/failure Alert Notification status.

To enable Alert Notification Status Tracking

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.
3. Select the **Enable Alert Notification Status** check box.

   You might receive notifications for the configured Alerts, but you may not be able to track the success/failure status of those notifications if you disable this option.
4. Click **OK**.

   EventTracker displays the confirmation message box.
5. Click **Yes** to save the changes.
6. Open the Reports Console, Click the Reports tab, click the Operations tab and then click XYZ to configure the report.

   Reports Console generates the report without data, had you disabled this option.

Purging Alert Events Cache

This option helps you purge Alert Events cache. By default, EventTracker retains event data for seven days. You can configure to hold minimum 24-hour and maximum 90 days event data. You cannot completely purge the cache.

To purge Alert Events Cache

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.
3. Select the **Enable Alert Events Cache for Alert Analysis** check box.

   EventTracker enable the **Purge events from cache older than** spin box.
4. Select the duration from the spin box.
5. Click **OK**.

   EventTracker displays the confirmation message box.
6. Click **Yes** to save the changes.

7 Open the Reports Console, Click the Analysis tab, click the Alerts analysis type to configure the report.

Reports Console generates the report for the configured number of days.

Show Only Active Alert events in Console

When you open the Management console, initially EventTracker sets focus on the Correlated Alerts & Incidents Category and displays all events occurred in that Category. To view only active Alerts, select the "Show only Active Alert events in Console" check box. When this check box is selected, EventTracker stores all Alert events in the database, but displays only the active Alerts on the Management Console. Since all Alert events are stored in the database, analysis could be done on all Alert events.

Note

Active Alerts are Alert events that have at least one action set.

To show only active Alert events in Console

1 Open the Management Console.

2 Click the **Configure** menu and select the **Configure Manager** option.

EventTracker displays the Manager Configuration window.

3 Select the **Show Only Active Alert events in Console** check box.

4 Click **OK**.

EventTracker displays the confirmation message box.

5 Click **Yes** to save the changes.

Store Only Active Alert events

To store only active Alerts, select the Store only Active Alert events check box. When this check box is selected, EventTracker stores only the active Alerts events in the database. Analysis could be done only on active Alert events. "Show only Active Alert events in Console" option is enabled by default, if you select this check box.

To store only active Alert events

1 Open the Management Console.

2 Click the **Configure** menu and select the **Configure Manager** option.

EventTracker displays the Manager Configuration window.

3 Select the **Store only Active Alert events** check box.

4 Click **OK**.

EventTracker displays the confirmation message box.

5 Click **Yes** to save the changes.

Enabling Remedial Actions

It is mandatory to enable remedial action at Manager Console. Otherwise you cannot execute remedial action at the Agent systems.

To configure remedial action

1 Open the Management Console.

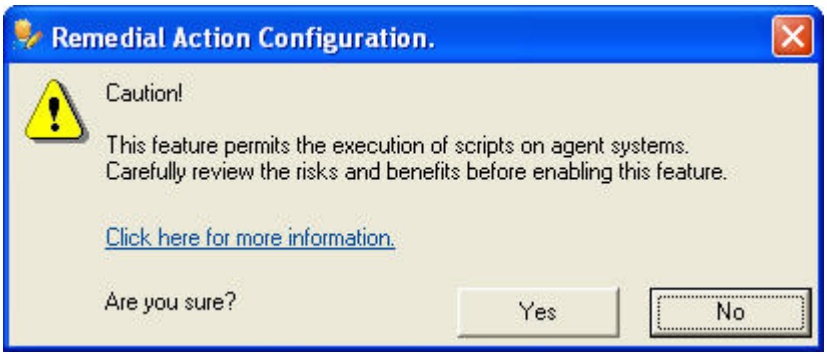
2 Click the **Configure** menu and then select the **Configure Manager** option.

EventTracker displays the Manager Configuration window.

3 Select the **Enable Remedial Action** check box.

EventTracker displays the Caution dialog box.

Figure 53 Remedial Action Configuration


Remedial Action Configuration.
Caution!
This feature permits the execution of scripts on agent systems.
Carefully review the risks and benefits before enabling this feature.
Click here for more information.
Are you sure?
Yes
No

4 Click **Yes**.

5 Click **OK** on the Manager Configuration window.

EventTracker displays confirmation dialog box to save changes.

6 Click **Yes**.

Suppressing Duplicate Alerts

What does "Duplicate Alert Suppression" mean?

EventTracker provides the facility of generating user configurable alerts for events received by the EventTracker. This feature is very useful in case the user is not always available at the Manager Console.

In case the multiple instances of an event with a configured alert are received in a short period of time then a large number of alerts will be generated, this could confuse the user.

Duplicate Alert Suppression feature will handle such a deluge of alerts by suppressing any alert in case it is a duplicate of an alert received earlier, within a particular time-frame.

How do I use the feature "Duplicate Alarm Suppression"?

The "Duplicate Alarm Suppression" feature is GUI driven. The configuration settings are present in the evtrxer.ini. This configuration file is located in the directory where the EventTracker is installed. Typical example would be: "C:\Program Files\Prism Microsystems\EventTracker"

The evtrxer.ini file has the following settings by default:

dup_suppr_interval = 0

max_alerts_allowed = 0

dup_suppr_interval: This is the interval during which duplicate alerts will be suppressed. The interval can be defined in seconds

- value 0 DISABLES the suppression feature.

max_alerts_allowed: This is the maximum number of duplicate alerts that will be allowed during the interval set in dup_suppr_interval.

- 0 value causes all duplicate alerts to be suppressed, which means that only one alert will be allowed during the Suppression Interval.

Note

The EventTracker Receiver service has to be restarted once any change is made to the evtrxer.ini file. If the service is not restarted the changes made will not be taken in by the service.

Sample Alert Suppression setting

dup_suppr_interval = 300

max_alerts_allowed = 5

The above settings inform the EventTracker to allow a MAXIMUM of 5 DUPLICATE alerts to be triggered within a timeframe of 300 seconds. An alert is considered a duplicate only if it is triggered by the same event.

This option helps you suppress duplicate Alerts.

To suppress duplicate Alerts

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.
3. Select the **Suppress Duplicate Alerts** check box.

   EventTracker displays **Alert suppression interval** and **Maximum number of alerts allowed** fields.
4. Type appropriately in the relevant fields.
5. Click **OK**.

   EventTracker displays the confirmation message box.
6. Click **Yes** to save the changes.

Configuring Manager to Alert Suspicious Network Activity

This option helps you receive Alert notification via different modes. EventTracker Manager generates and logs events whenever it detects suspicious network activity. To be notified of these events, you have to enable Suspicious Network Activity Alerts feature in the Manager Configuration console.

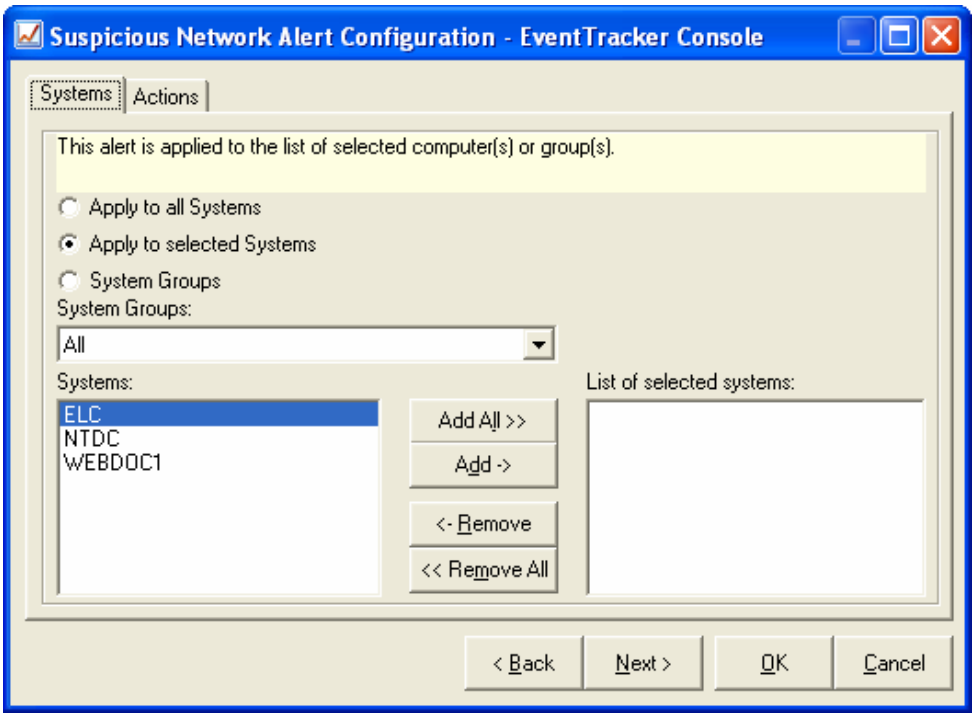
To configure Manager to alert Suspicious Network Activity

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.
3. Select the **Suspicious Network Activity** check box.

   EventTracker displays the Suspicious Network Alert Configuration console.

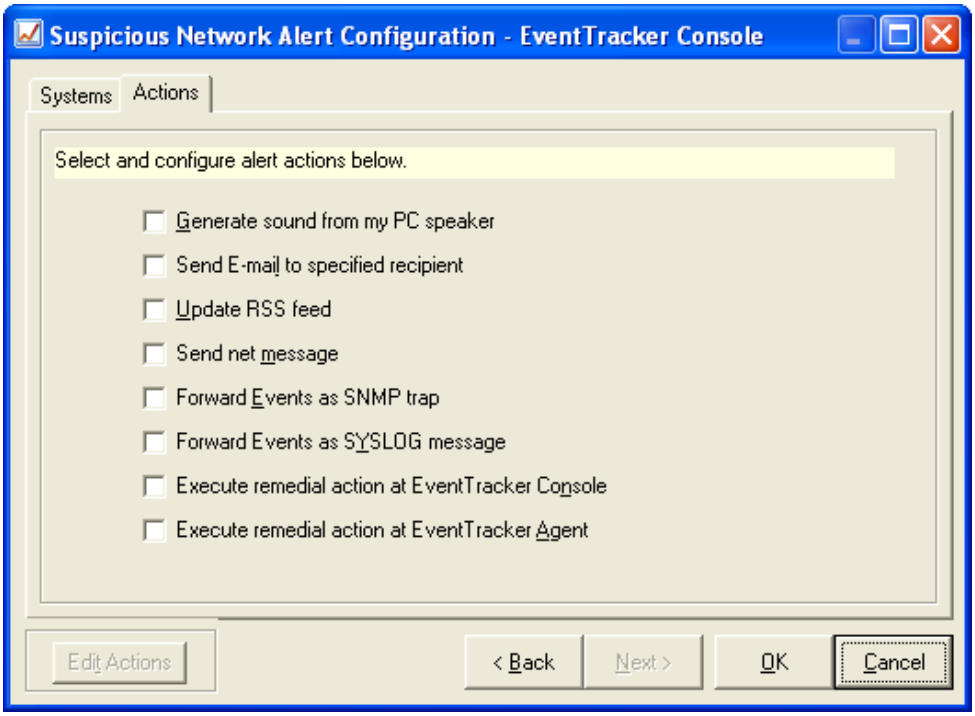
Figure 54 Suspicious Network Alert Configuration



4. Select Groups / Systems and then click **Next>**.

   EventTracker displays the Actions tab.

Figure 55 Suspicious Network Alert Configuration



5 Select appropriate alert actions and then click **OK**.

6 Select the **Check to Knowledge base updates** check box.

7 Click **OK** on the Manager Configuration window.

EventTracker displays the confirmation message box.

8 Click **Yes** to save the changes.

Note

By selecting Check for Knowledge base updates, EventTracker updates the latest **Suspicious_Ports.ini** file by downloading from EventTracker Knowledge Base Web site. Suspicious_Ports.ini file contains blacklisted applications and ports, which are known threats to any enterprise setup. When you generate Network Analysis report EventTracker fetches apt suggestions from this file and displays in the report. Although selection of Check for Knowledge base updates check box is an option, it is advisable to update this file.

Chapter 4
Configuring Alerts and Alert Notifications

In this chapter, you will learn how to:

- Configure Alerts
- Configure Alert Actions
- Configure Remedial Actions

Alerts

EventTracker generates an alert when a critical event occurs, such as security breaches, performance problems, etc. Configure an unlimited number of rule-based alerts with customizable event criteria including support for event-fired automatic (custom) actions for any defined event.

- Out of the Box Alerts for the most common predefined alert condition.
- Ability to create your own alert conditions.
- Reliable framework for alerts.
- Ability to minimize false positive.
- Firing automatic actions as a receipt of event can increase system's availability.

Configuring Alerts

This option enables you to configure Alert Groups, add events to Alert Groups, and configure Alert Actions.

To configure Alerts

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Alerts** option.

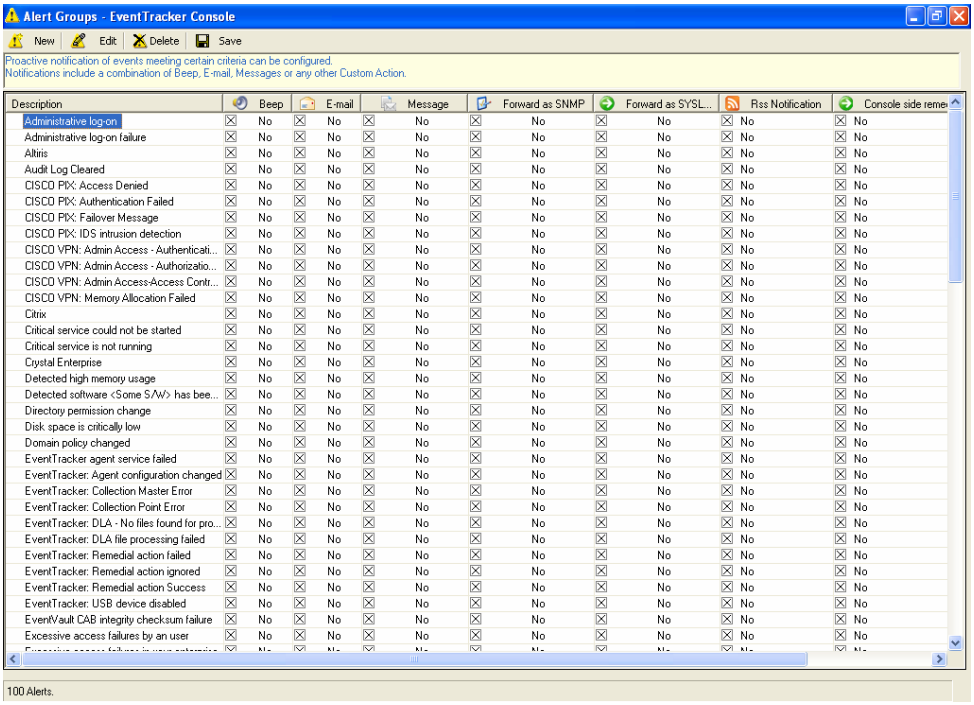
   (OR)

   Open the Alerts Dashboard.

   Click the **Alert Config** hyperlink in the right-upper corner.

   EventTracker displays the Alert Groups console.

Figure 56 Alert Groups



3 Right-click the Category that you want to set as alert in the Management Console.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Add As Alert**

(OR)

Open the Manage Categories console.

Right-click the Category that you want to set as Alert.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Add As Alert**

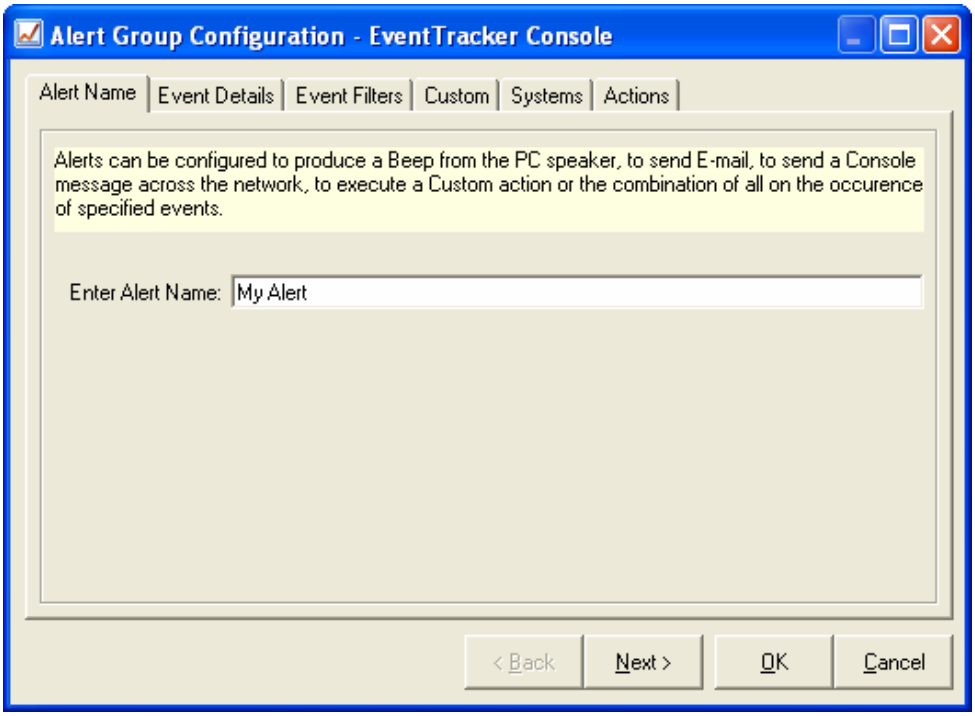
(OR)

Click **New** on the toolbar.

EventTracker displays the Alert Group Configuration window.

4 Type the Alert name in the **Enter Alert Name** field.

Figure 57 Alert Group Configuration – Alert Name tab


Alert Group Configuration - EventTracker Console
Alert Name
Event Details
Event Filters
Custom
Systems
Actions
Alerts can be configured to produce a Beep from the PC speaker, to send E-mail, to send a Console message across the network, to execute a Custom action or the combination of all on the occurence of specified events.
Enter Alert Name:
My Alert
< Back
Next >
OK
Cancel

5 Click the **Event Details** tab.

(OR)

Click **Next>**.

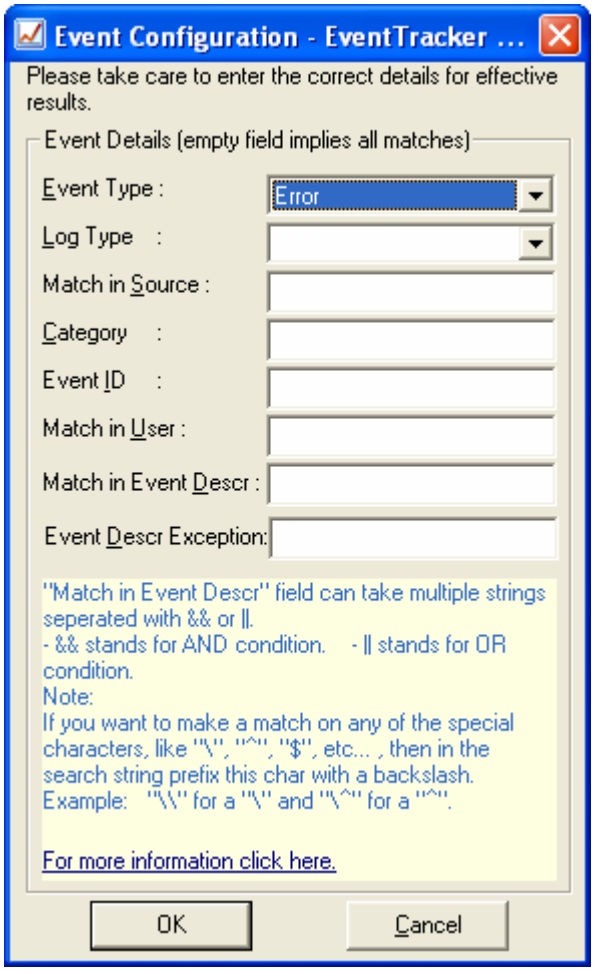
EventTracker displays the Event Details tab.

6 Click **Add Event**.

EventTracker displays the Event Configuration dialog box.

7 Type appropriately in the relevant fields.

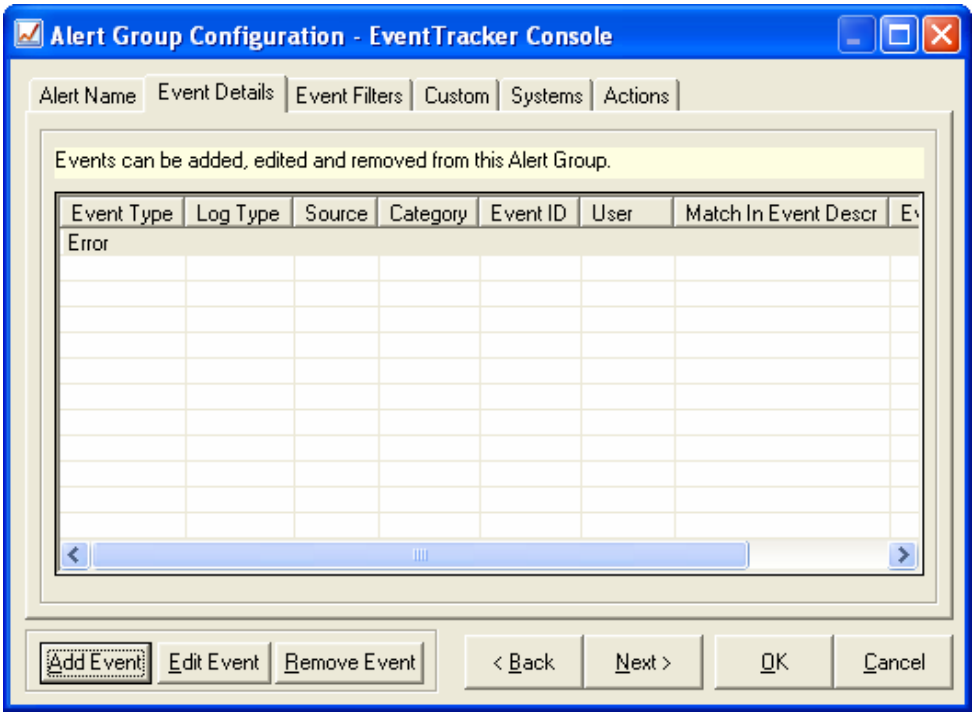
Figure 58 Event Configuration


Event Configuration - EventTracker ...
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Event Type :
Error
Log Type :
Match in Source :
Category :
Event ID :
Match in User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

8 Click **OK**.

EventTracker displays the Event Details tab with newly added Event details.

Figure 59 Alert Group Configuration – Event Details tab



9 Select an event from the list. Click **Edit Event** to modify and **Remove Event** to delete the settings.

10 Click the **Event Filters** tab.

(OR)

Click **Next>**.

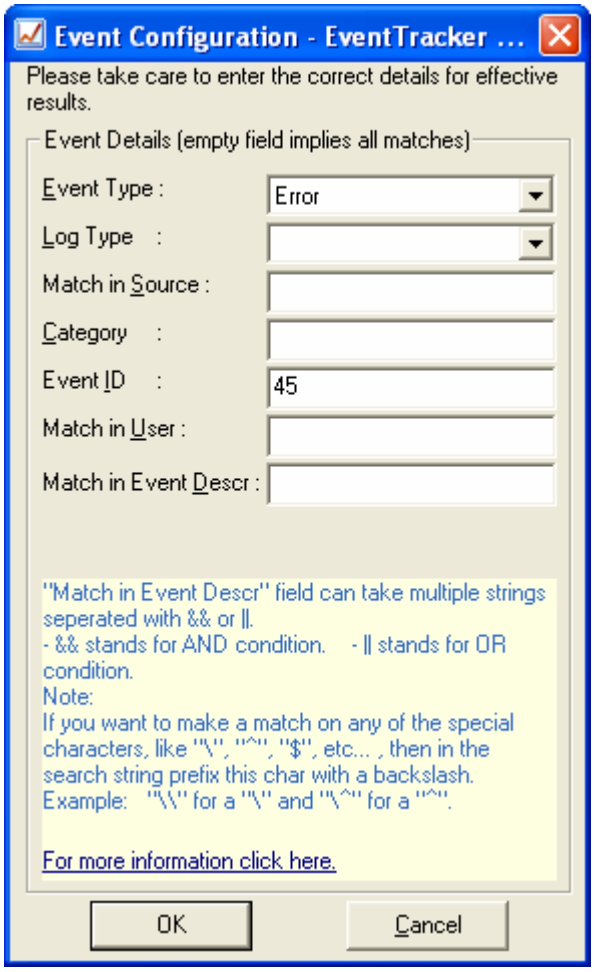
EventTracker displays the Event Filters tab.

11 Click **Add Event**.

EventTracker displays the Event Configuration dialog box.

12 Type appropriately in the relevant fields.

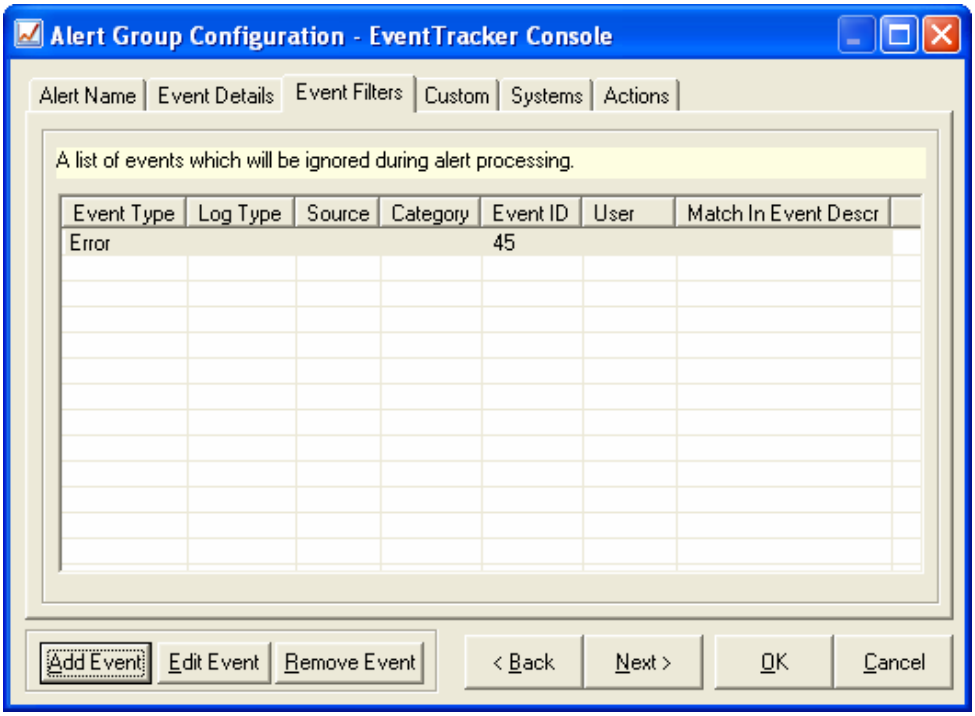
Figure 60 Event Configuration


Event Configuration - EventTracker ...
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Event Type :
Error
Log Type :
Match in Source :
Category :
Event ID :
45
Match in User :
Match in Event Descr :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

13 Click **OK**.

EventTracker displays the Event Filters tab with the newly added event filter.

Figure 61 Alert Group Configuration – Event Filters tab



14 Click the **Custom** tab.

(OR)

Click **Next>**.

EventTracker displays the Custom tab.

Figure 62 Alert Group Configuration – Custom tab

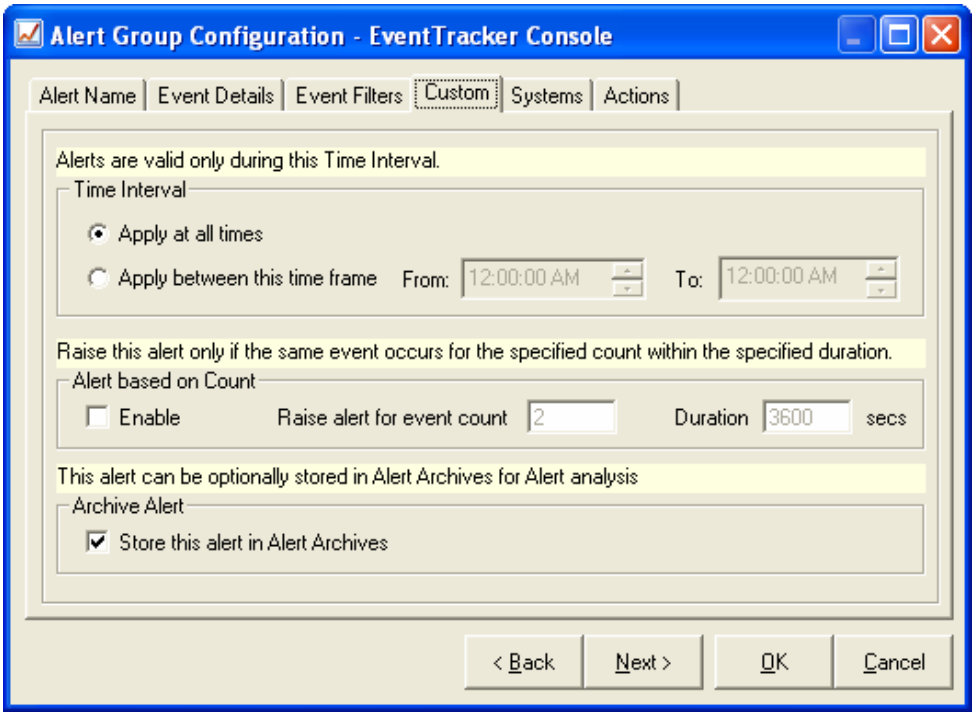
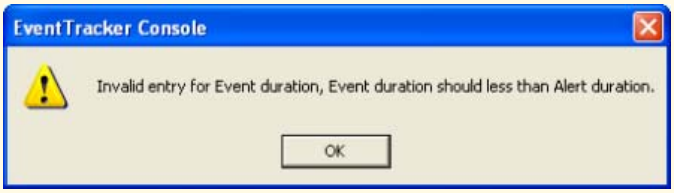


Table 18

Field	Description
Apply at all times	EventTracker selects this option by default and sends Alert notification whenever the specified events occur.
Apply between this time frame	Select this option when you want Alert notification on the occurrence of specified events within a specified time frame.
Alert based on Count	This option lets you to receive Alert notification only when the specified events occur for a specified number of times within the specified duration. EventTracker disables **Raise alert for event count** and **Duration** fields by default. To enable, select the **Enable** check box below. The default value for Raise Alert for event count is 2 and Duration is 3600 secs. When you select the **Apply between this time frame** option and type From and To times, EventTracker automatically updates the Duration seconds. You are not permitted to set the seconds beyond this limit. If you try EventTracker displays the EventTracker Console message and insists you to Type valid duration seconds. 

Field	Description
Archive Alert	Select this check box to store the Alert in the Alerts Archive for Alert analysis.

15 Select the **Apply between this time frame** option.

16 Select **From** and **To** time from the spin boxes.

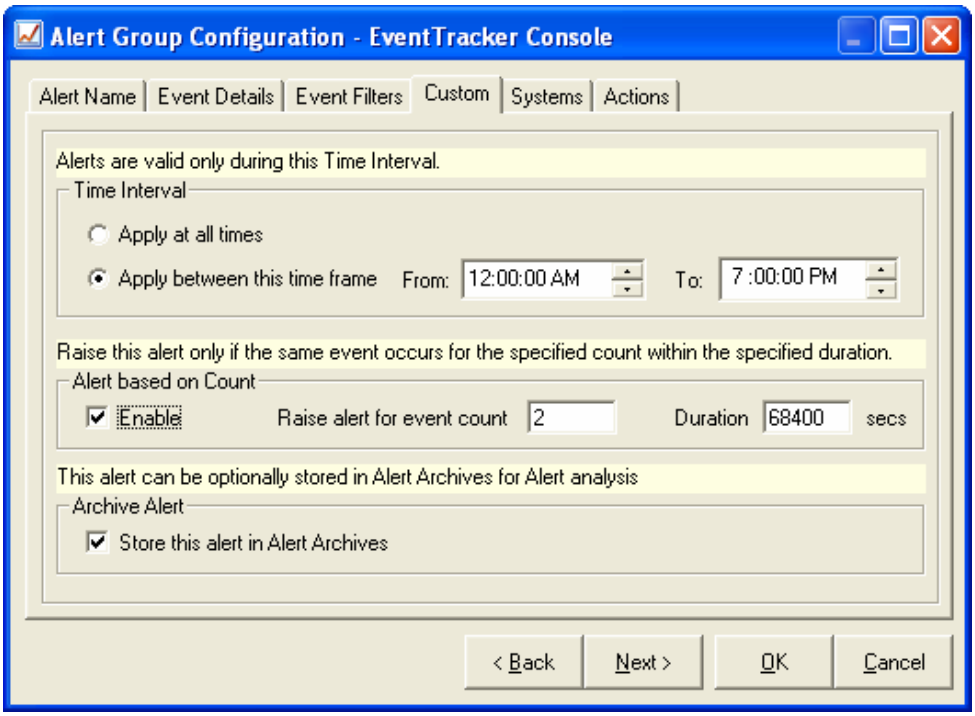
17 Select the **Alert based on Count** check box.

18 Type the count in the **Raise alert for event count** field.

19 Type the secs in the **Duration** field.

EventTracker displays the Custom tab with newly added custom settings.

Figure 63 Alert Group Configuration – Custom tab



20 Click the **Systems** tab.

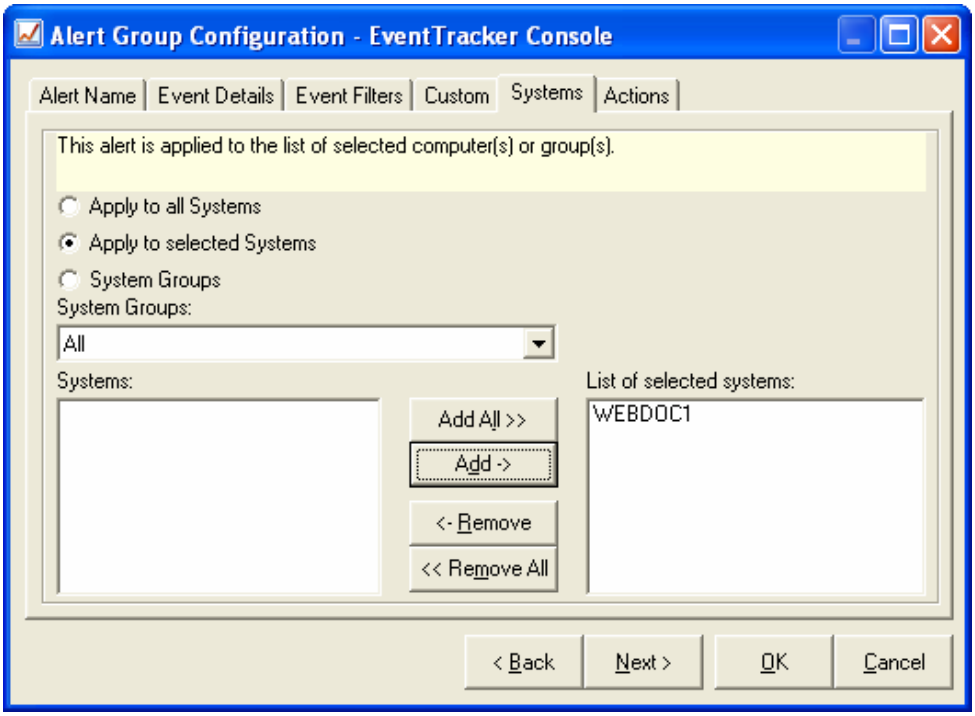
(OR)

Click **Next>**.

EventTracker displays the Systems tab.

21 Select the System Groups / Systems.

Figure 64 Alert Group Configuration – Systems tab



22 Click the **Actions** tab.

(OR)

Click **Next>**.

EventTracker displays the Actions tab.

Figure 65 Alert Group Configuration – Actions tab

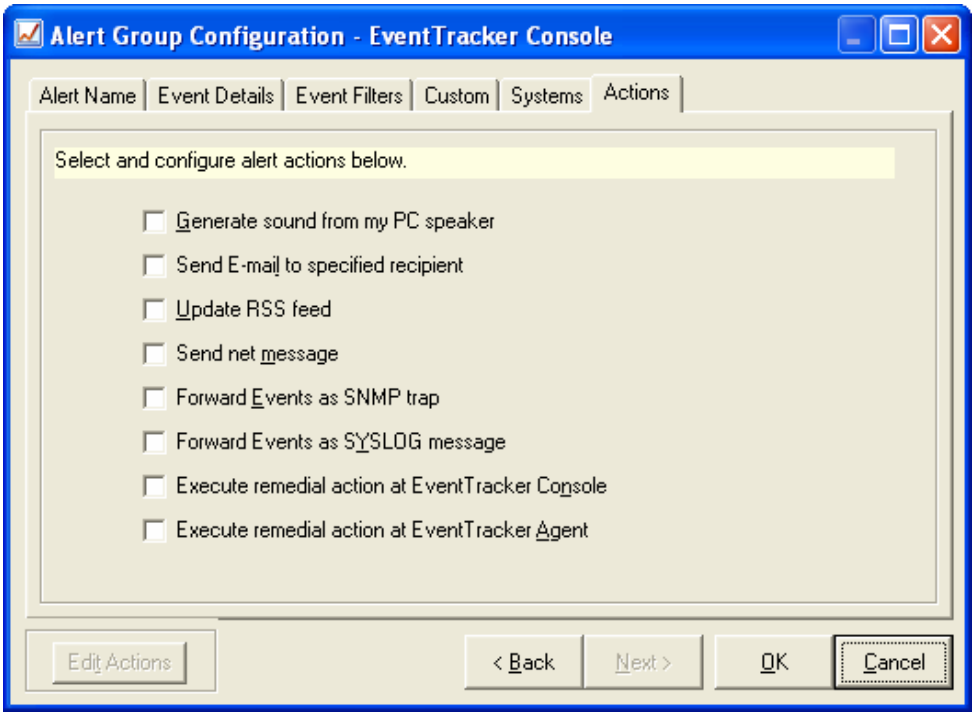


Table 19

Field	Description
Generate sound from my PC speaker	Select this option to configure audible Alert notification.
Send E-mail to specified recipient	Select this option to configure E-mail Alert notification.
Update RSS feed	Send Alerts via RSS Feeds.
Send net message	Select this option to configure console message notification.
Forward Events as SNMP trap	Select this option to forward events as SNMP trap.
Forward Events as SYSLOG messages	Select this option to forward events as SYSLOG message.
Execute Remedial action at EventTracker	Select this option to configure custom action to be executed on receipt of an event at the Manager side.

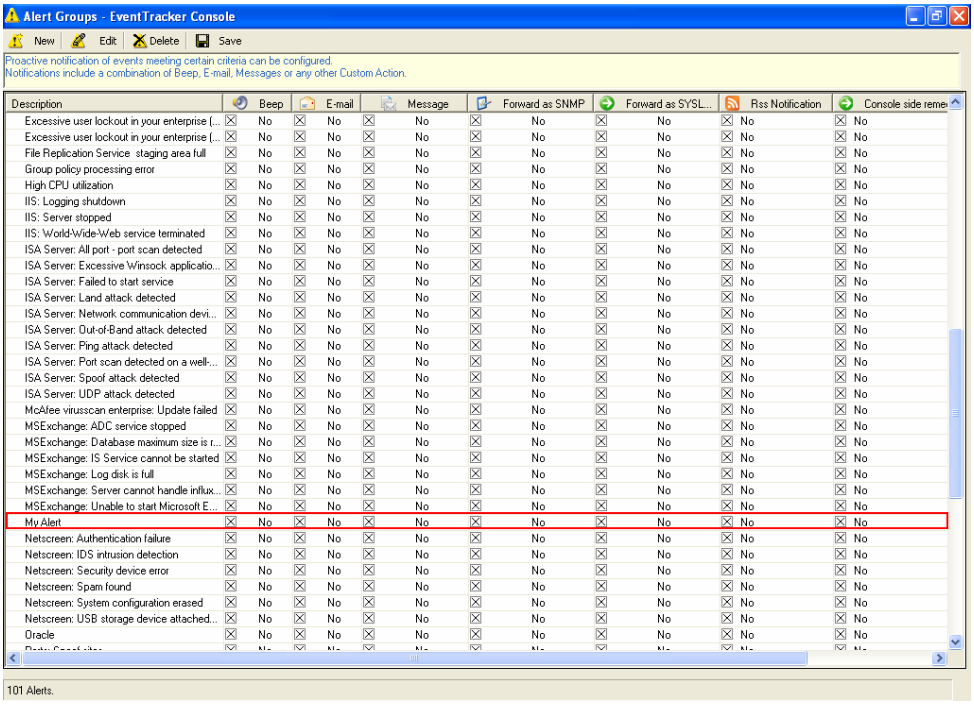
Field	Description
console	
Execute Remedial action at EventTracker Agent	Select this option to configure custom action to be executed on receipt of an event at the Agent side. You execute these actions only on Windows systems where agents are deployed. You cannot execute these actions on NIX systems where Agent less monitoring is deployed.

23 Select the type of action and type appropriate information in the displayed dialog boxes.

24 Click **OK**.

EventTracker displays the Alert Groups console with the newly added Alert Group.

Figure 66 Alert Groups



25 Click **Save** on the toolbar.

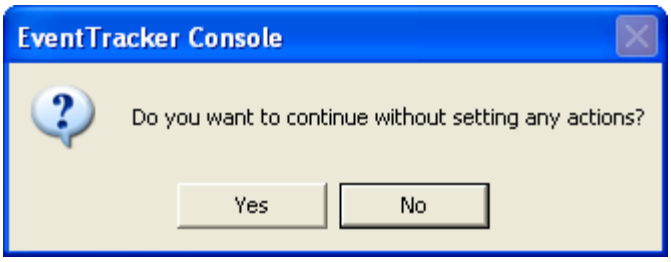
EventTracker displays EventTracker Management Console Message.

26 Click **OK**.

27 Restart the Management Console.

EventTracker displays the EventTracker Console message box, have you not chosen any actions in the Alert Group Configuration – EventTracker Console.

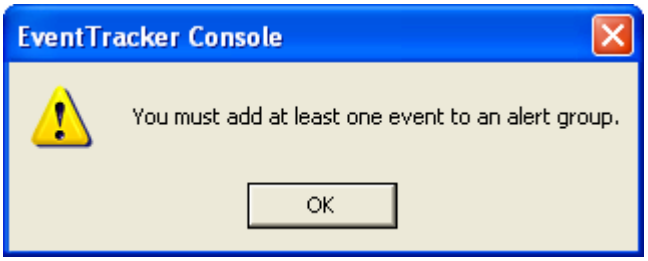
Figure 67
EventTracker Console message box



28 Click **Yes** to set the actions later.

EventTracker displays EventTracker Console message box, have you not added Event Details.

Figure 68
EventTracker Console message box



Managing Categories

1 Right-click any Category Group in the **All Categories** hive in the Management Console.

EventTracker displays the shortcut menu.

From the shortcut menu, choose the **Manage Categories** option.

EventTracker displays the Manage Categories console.

Expand the **All Categories** hive.

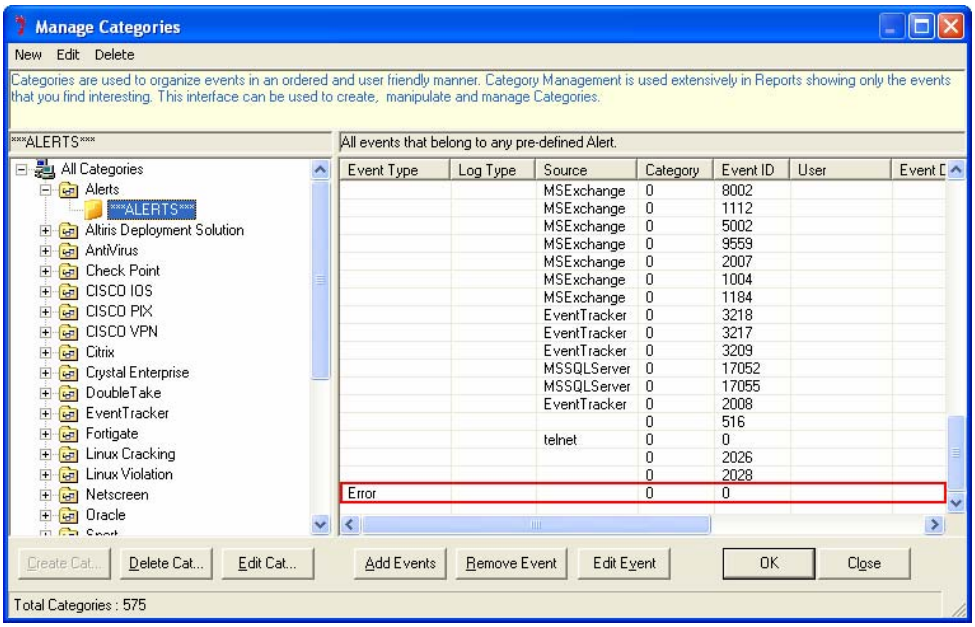
Expand the **Alerts** Group.

Click the **Alerts Category**.

2 Scroll the right pane.

EventTracker adds the events configured for the new Alert (**My Alert**) along with the predefined events.

Figure 69 Manage Categories console



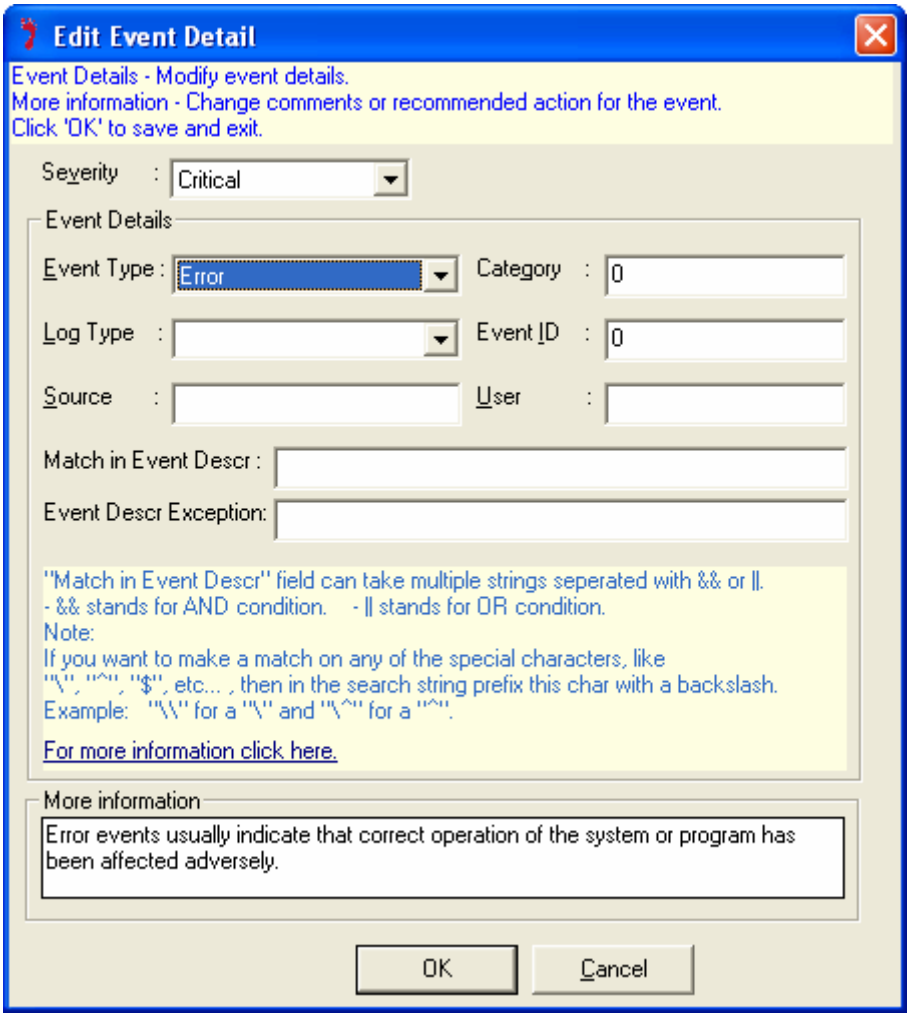
Note

You can edit and delete the new event details in ***Alerts*** Category. These manipulations would not affect the event details of the new Alert that is My Alert in the Alert Groups console.

3 Click **Edit Event**.

EventTracker displays the Edit Event Detail window.

Figure 70 Edit Event Detail

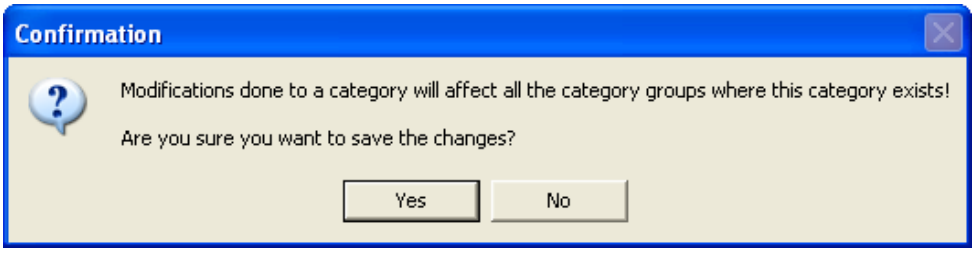

Edit Event Detail
Event Details - Modify event details.
More information - Change comments or recommended action for the event.
Click 'OK' to save and exit.
Severity : Critical
Event Details
Event Type : Error
Category : 0
Log Type :
Event ID : 0
Source :
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
Error events usually indicate that correct operation of the system or program has been affected adversely.
OK
Cancel

4 Type appropriately in the relevant fields. Example: Log Type: Application.

5 Click **OK**.

EventTracker displays the Confirmation message box.

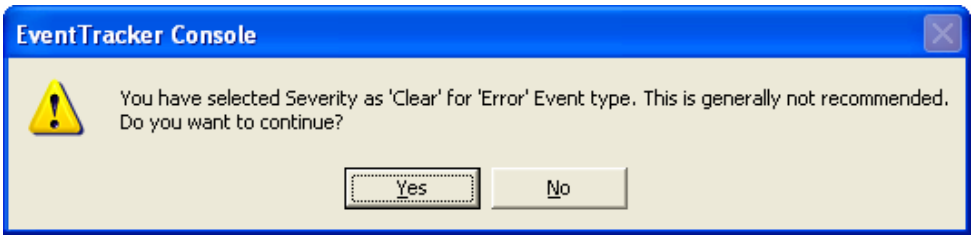
Figure 71 Confirmation message box


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

6 Click **Yes**.

EventTracker displays the EventTracker Console message box, if there is disparity in Severity and Event Type.

Figure 72
EventTracker Console message box

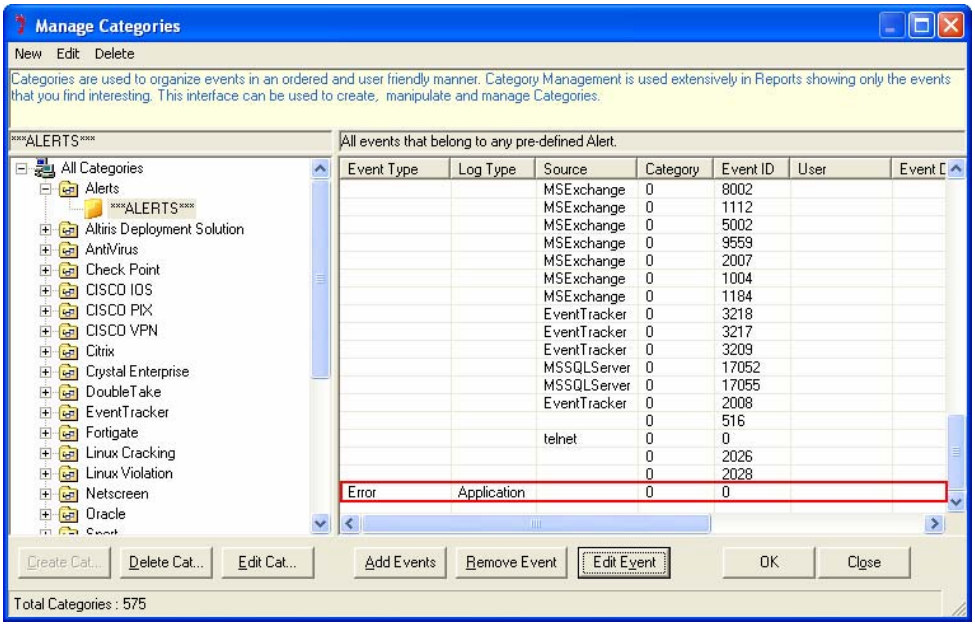

EventTracker Console
You have selected Severity as 'Clear' for 'Error' Event type. This is generally not recommended. Do you want to continue?
Yes
No

7 Click **No**.

8 Select appropriate severity from the **Severity** drop-down list.

EventTracker displays the Manage Categories console with the modified event details.

Figure 73 Manage Categories console



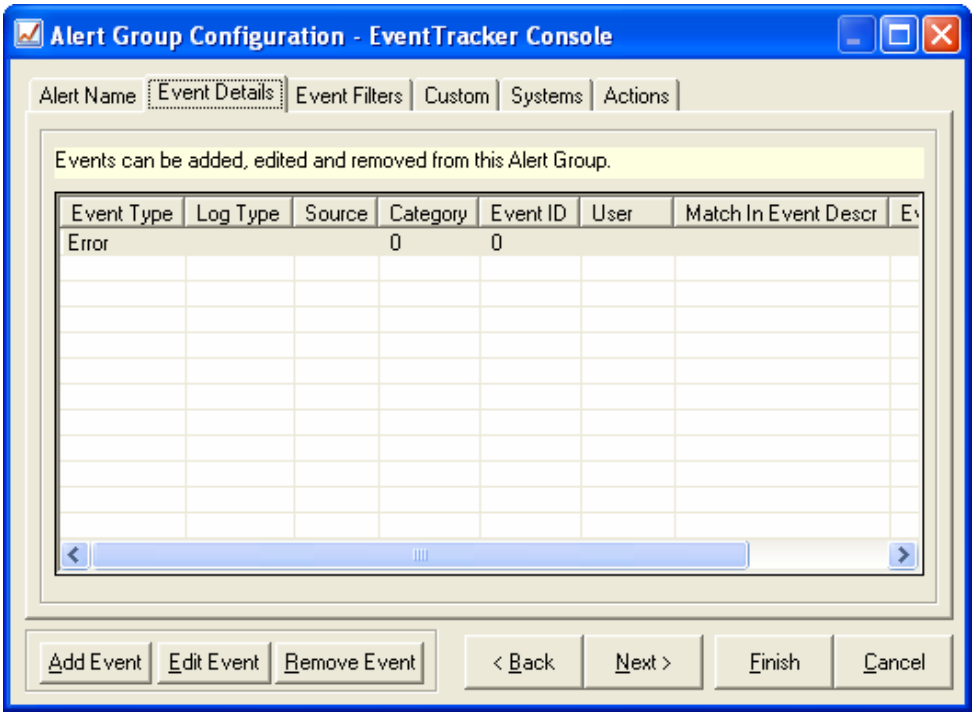
9 Click **OK**.

10 Open **Alert Groups** console.

11 Double-click **My Alert**.

EventTracker displays the Event Details tab with event details unaltered.

Figure 74 Alert Group Configuration



Note

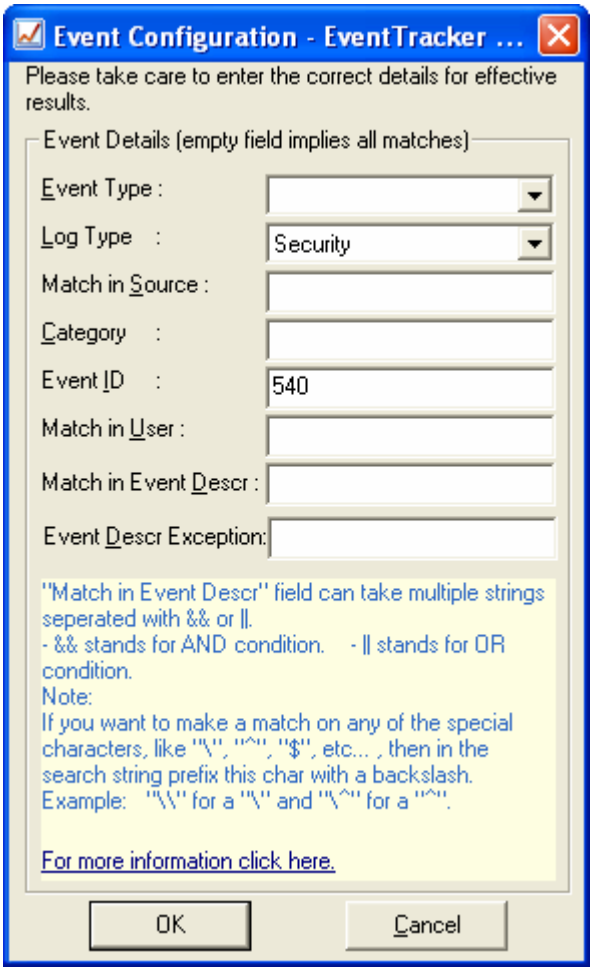
However, when you edit the event details of My Alert in Alert Group Configuration window, it will be reflected in ***Alerts*** Category in the Manage Categories console.

12 Double-click the event or click **Edit Event**.

EventTracker displays the Event Configuration window.

13 Type appropriately in the relevant fields.

Figure 75 Event Configuration


Event Configuration - EventTracker ...
Please take care to enter the correct details for effective results.
Event Details (empty field implies all matches)
Event Type :
Log Type :
Security
Match in Source :
Category :
Event ID :
540
Match in User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
OK
Cancel

14 Click **OK**.

EventTracker displays the Alert Group Configuration window with the modified event details.

15 Click **Finish**.

16 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

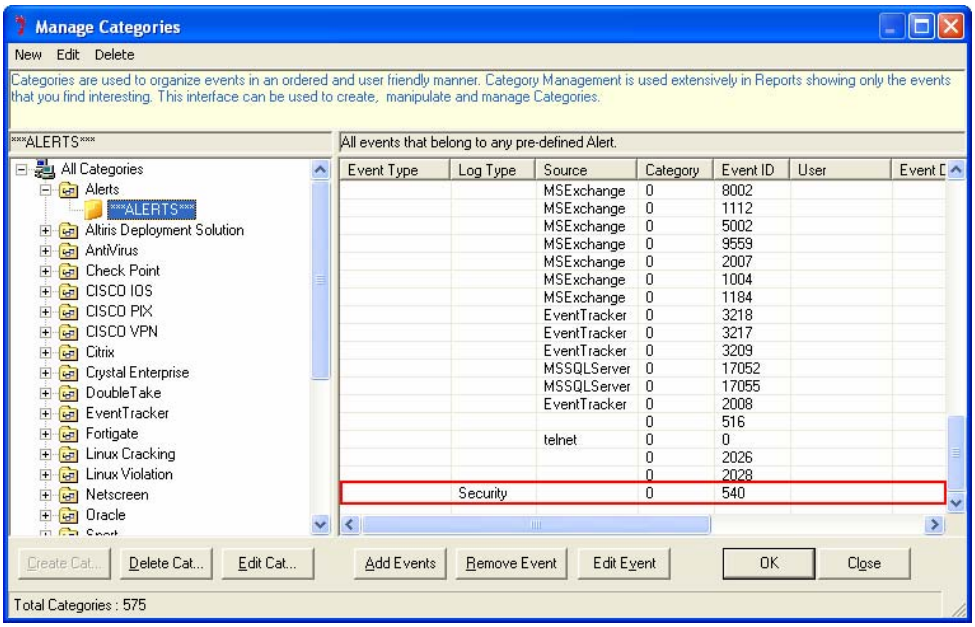
17 Click **OK**.

18 Restart the Management Console.

19 Open the Manage Categories console.

EventTracker displays the modified event details of My Alert.

Figure 76 Manage Categories console



Note

The advantages of adding new Alert Group's event details along with the event details of pre-defined *****Alerts***** Category are as follows:

- Apart from alert notifications, reports can be generated for the new Alerts along with the pre-defined ***Alerts*** Category.
- Event analysis can be done for the newly added Alerts.
- Event severity for the new Alerts can be viewed in the Navigation pane etc.,

Modifying Alert Details

This option enables you to modify the Alert details.

To modify Alert details

1. Open the **Alert Groups** console.

   EventTracker displays the Alert Groups console.

2. Select the Alert from the list (ex: **My Alert**)

3 Click **Edit** on the toolbar.

(OR)

Double-click the Alert.

EventTracker displays the Event Details tab on Alert Group Configuration dialog box.

Note

The **Event Details** tab selected by default and the **Alert Name** is non-editable but you can view the Alert Name.

4 Select the event that you want to modify.

Click **Edit Event**.

(OR)

Click **Edit** on the toolbar.

(OR)

Double-click the event.

EventTracker displays the Event Configuration dialog box.

5 Type appropriately in the relevant fields.

6 Click **OK**.

EventTracker displays the Event Details tab on Alert Group Configuration dialog box.

7 Click **Finish**.

EventTracker displays the EventTracker Console message box.

8 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

9 Click **OK**.

10 Restart the Management Console.

Deleting Alert Details

This option enables you to delete Alert details.

To delete Alert details

1 Open the **Alert Groups** console.

EventTracker displays the Alert Groups console.

2. Select the Alert that you want to delete from the list.
3. Click **Delete** on the toolbar.

   EventTracker displays the EventTracker Console confirmation message box.
4. Click **Yes**.
5. Click **Save** on the toolbar.

   EventTracker displays the EventTracker Management Control Message.
6. Click **OK**.
7. Restart the Management Console.

Configuring Alert Actions – Manager Side

This option enables you to configure Alert actions that are to be executed at the EventTracker Manager system.

To configure Alert actions

1. Open the Management console.
2. Click the **Configure** menu and select the **Configure Alerts** option.

   EventTracker displays the Alert Groups console.
3. Click **New** on the toolbar.

   EventTracker displays the Alert Group Configuration dialog box.
4. Type appropriately in the **Alert Name**, **Event Details**, **Event Filters**, **Time Interval** and **Computers** tabs.

Configuring Audible Alert Action

This option enables you to configure audible Alert action.

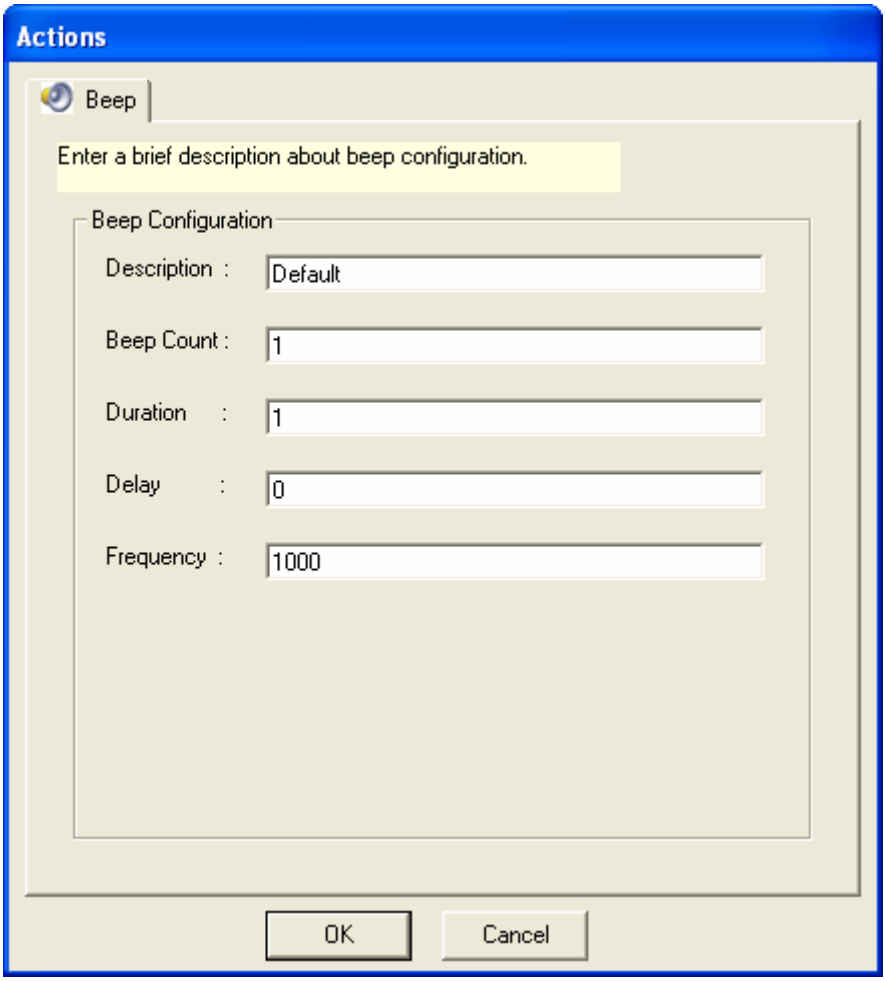
To configure audible Alert action

1. Click the **Actions** tab.

   EventTracker displays the Actions tab.
2. Select the **Generate sound from my PC speaker** check box.

   EventTracker displays the Actions-Beep dialog box.

Figure 77 Actions - Beep



Note

You can also access the Actions-Beep dialog box by selecting the corresponding check box under Beep column on the Alerts Group dialog box.

Table 20

Field	Description
Beep Configuration	
Description	Type the beep alert description in this field.
Beep Count	Type the number of beeps in this field. This field supports numeric data type only.

Field	Description
Duration	Type the duration in seconds in this field. This field supports numeric data type only.
Delay	Type the delay in seconds between beeps in this field. This field supports numeric data type only.
Frequency	Type the frequency in Hertz in this field. This field supports numeric data type only.

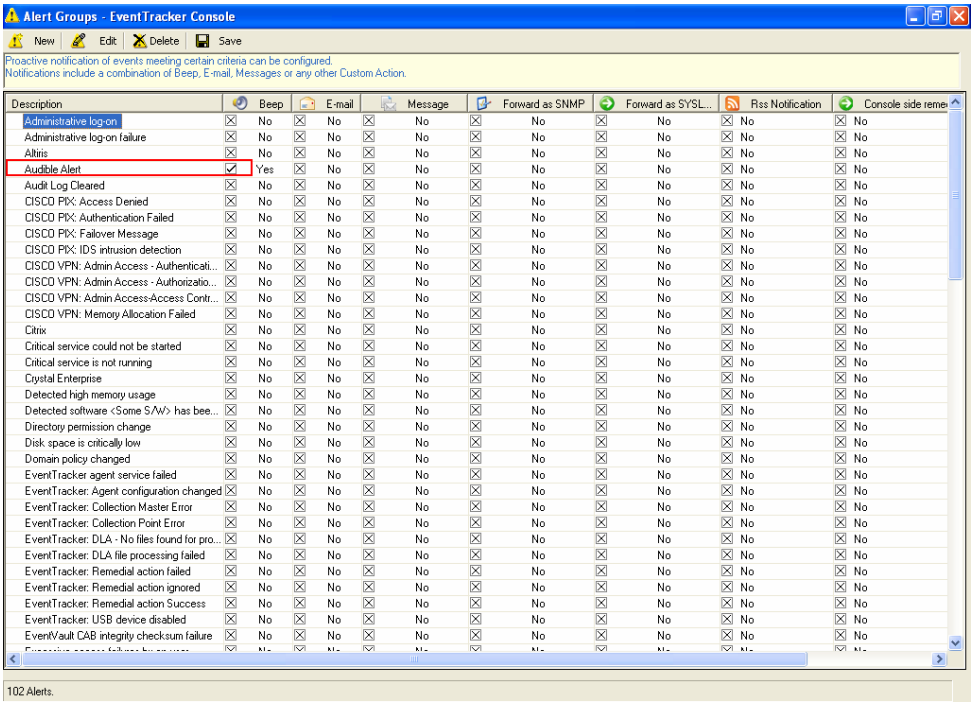
3 Type appropriately in the relevant fields.

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration window.

EventTracker displays the Alert Groups console with the newly created audible alert.

Figure 78 Alert Groups console



6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Configuring E-mail Alert Action

This option enables you to configure E-mail Alert action.

To configure E-mail Alert action

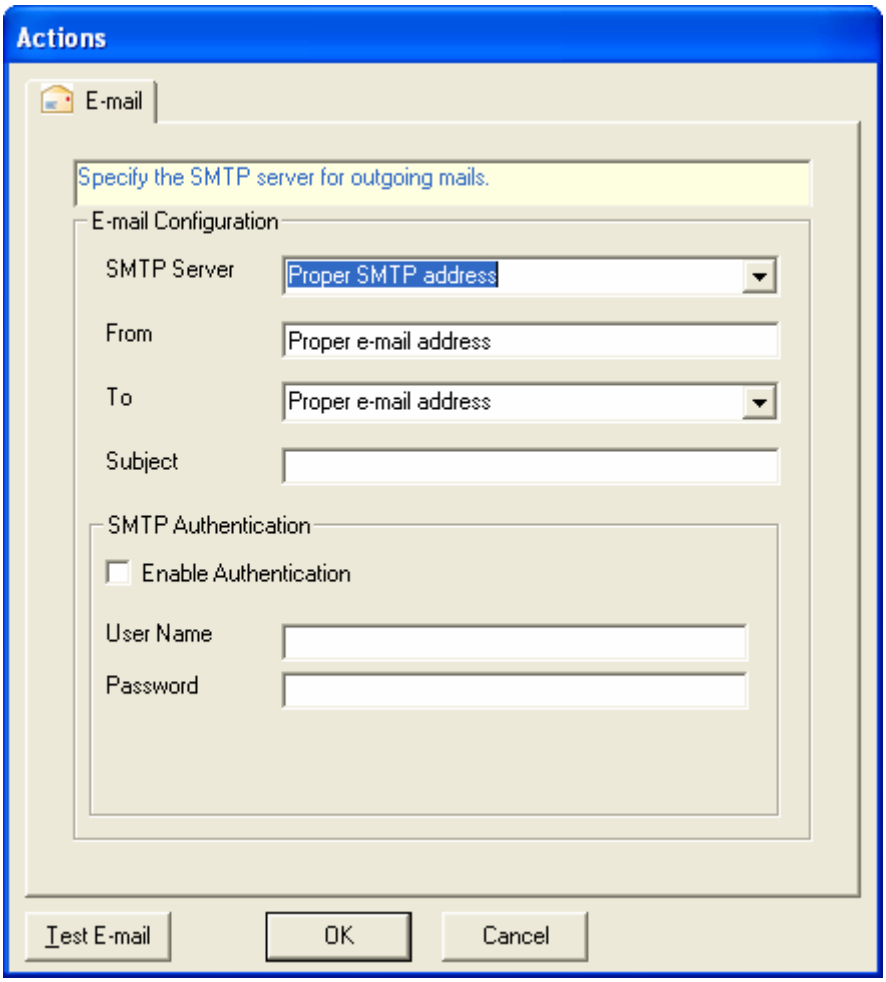
1. Click the **Actions** tab.

   EventTracker displays the Actions tab.

2. Select the **Send E-mail to specified recipient** check box.

   EventTracker displays the Actions-Email dialog box.

Figure 79 Actions - Email



Note

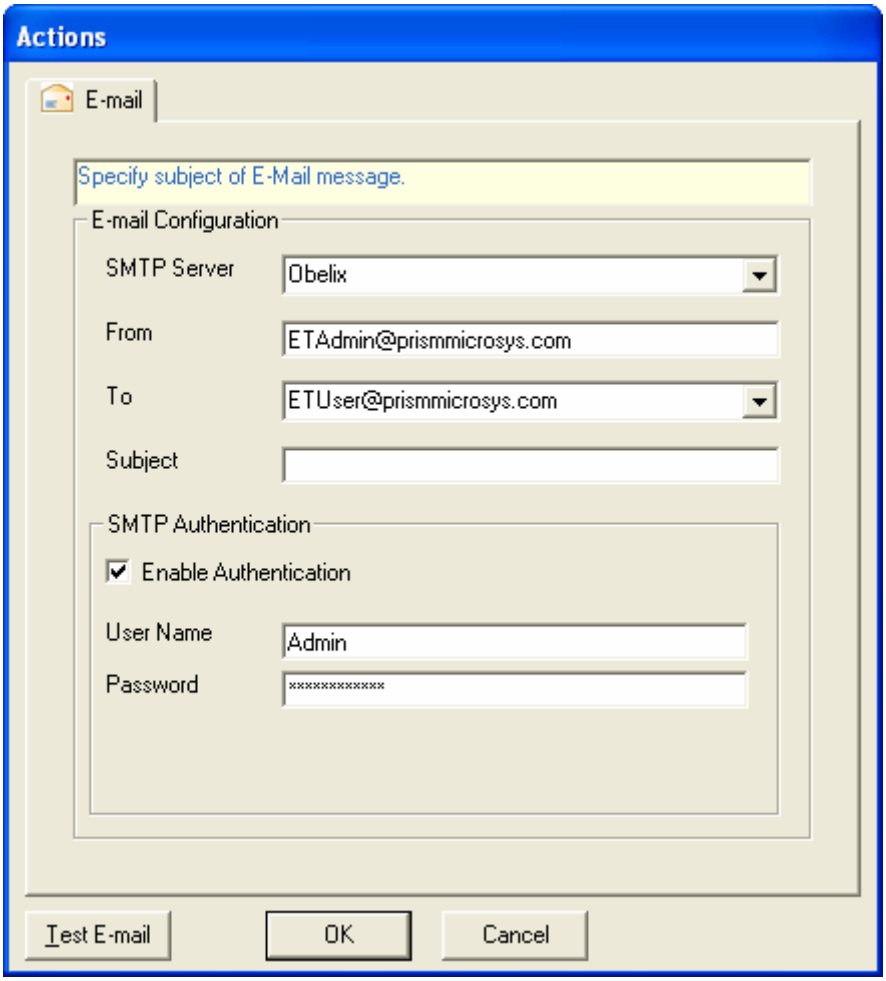
You can also access the Actions-Email dialog box by selecting the corresponding check box under **Email** column on the Alerts Group dialog box.

Table 21

Field	Description
E-mail Configuration	
SMTP Server	Type the SMTP Server name or select a SMTP Server from the drop-down list.
From	Type a valid sender E-mail address.
To	Type a valid recipient E-mail address. or select recipient E-mail address from the drop-down list.
Subject	Type the subject in this field.
SMTP Authentication: Provides an access control mechanism. It can be used to allow legitimate users to relay mail while denying relay service to unauthorized users, such as spammers.	
Enable Authentication	Select this check box to enable the SMTP Server authentication.
User Name	Type a valid username in this field.
Password	Type the password in this field.

3 Type appropriately in the relevant fields.

Figure 80 Actions - Email

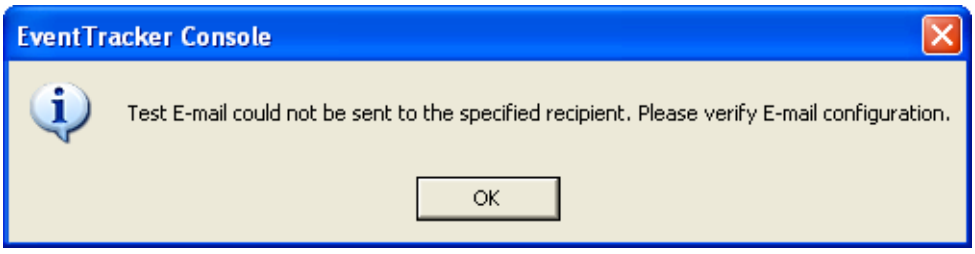


4 Click **OK**.

5 To test the E-mail configuration, click **Test Email**.

EventTracker displays the EventTracker Console message box, had you misconfigured the settings.

Figure 81 EventTracker Console – message box



6 Click **OK**.

EventTracker displays the EventTracker Console message box, had you properly configured the settings.

Figure 82
EventTracker Console – message box

EventTracker Console
Test E-mail has been sent to the specified recipient. Please verify whether the test E-mail has been received or not.
OK

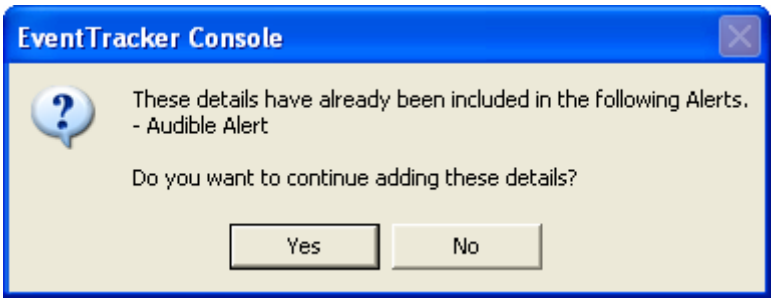
7 Click **OK**.

8 Click **OK** on the Actions-Email dialog box

9 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the EventTracker Console message box, if alert notification has been set previously for the same event details.

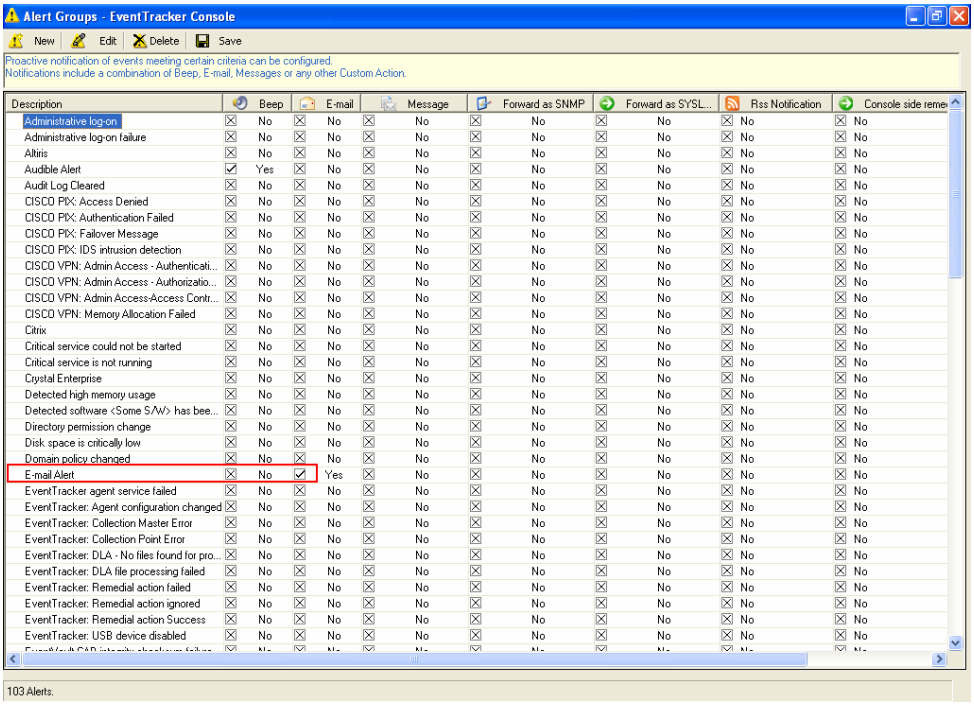
Figure 83
EventTracker Console – message box


EventTracker Console
These details have already been included in the following Alerts.
- Audible Alert
Do you want to continue adding these details?
Yes
No

10 Click **Yes** to continue or **No** to abort.

EventTracker displays the Alert Groups console with the newly created E-Mail alert.

Figure 84 Alert Groups console



11 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

12 Click **OK**.

13 Restart the Management Console.

I SETUP AN EMAIL ALERT AND IT IS NOT WORKING. WHAT SHOULD I DO?

Please crosscheck the following.

- The SMTP server mentioned must be accessible from the Console system. That is either the system must be able to access Internet or the SMTP server must be reachable over the LAN.
- Ensure valid email ids are provided in both "To Address" and "From Address". Note, the email ids MUST be valid.
- Try out the Test E-mail option provided where you are configuring the email.

Configuring Console Message Alert Action

This option enables you to configure a console message Alert. A notification message will be sent to the selected machine.

To configure console message Alert action

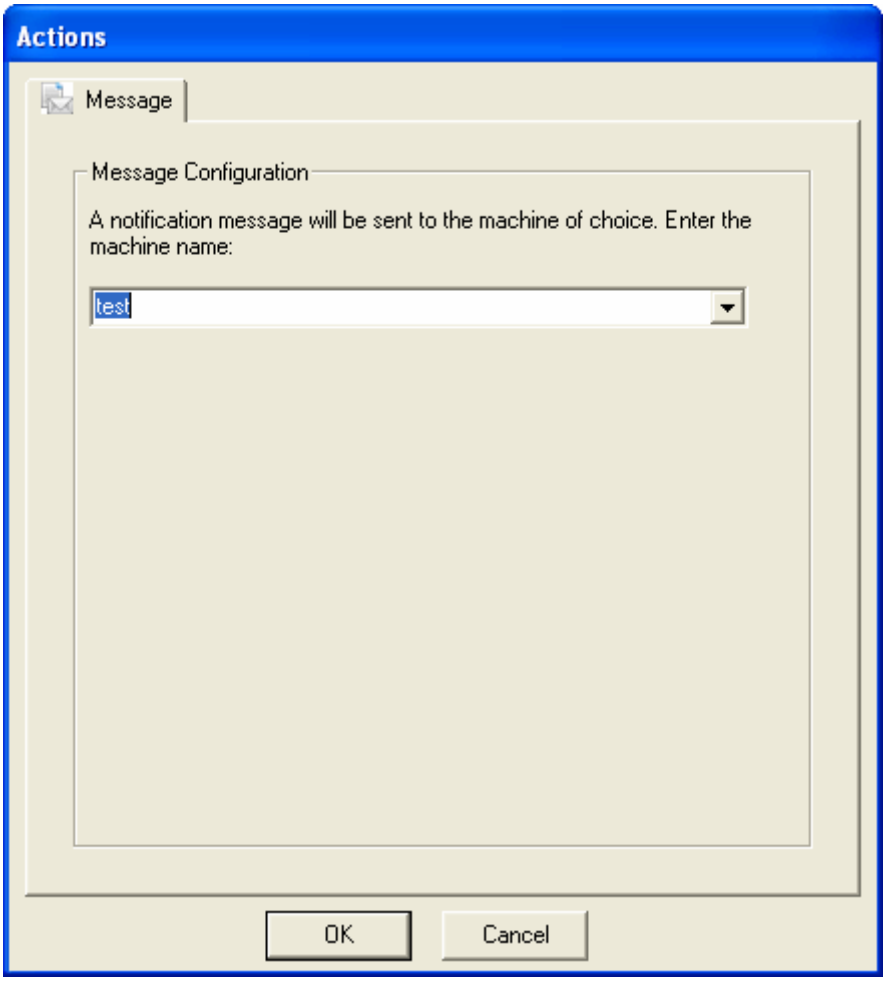
1. Click the **Actions** tab.

   EventTracker displays the Actions tab.

2. Select the **Send net message** check box.

   EventTracker displays the Actions-Message dialog box.

Figure 85 Actions - Message



Note

You can also access the Actions-Message dialog box by selecting the corresponding check box under Message column on the Alerts Group dialog box.

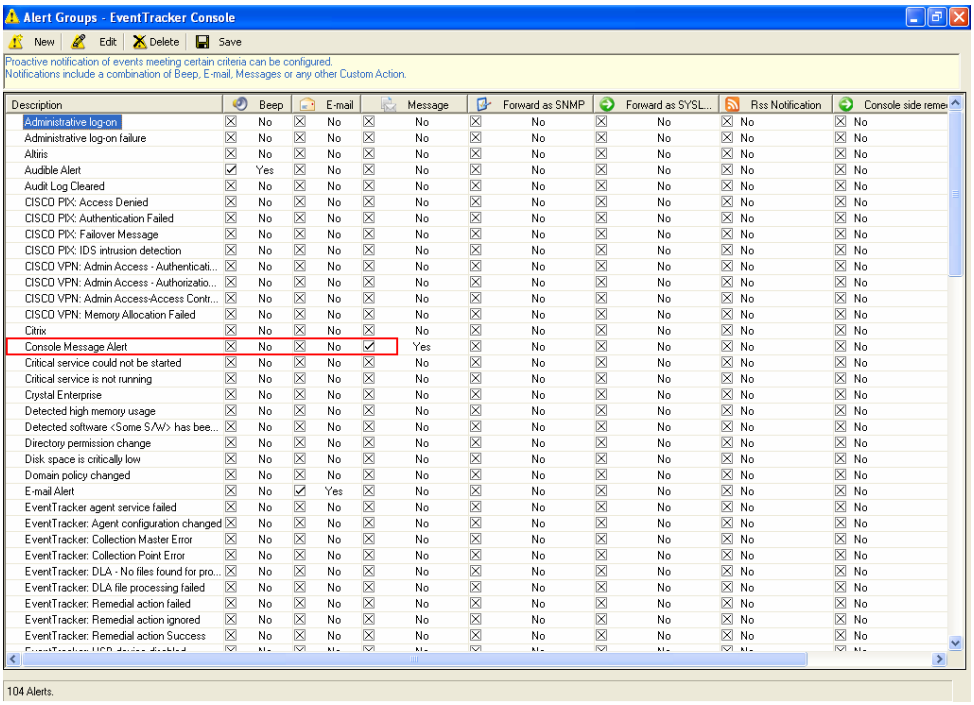
3 Type the system name under Message Configuration or select the system from the drop-down list.

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the Alert Groups console with the newly created console message alert.

Figure 86 Alert Groups console



6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Configuring RSS Alert Notification

This option helps you to get notified via RSS, Alerts raised by EventTracker for configured events.

To configure RSS Alert notification

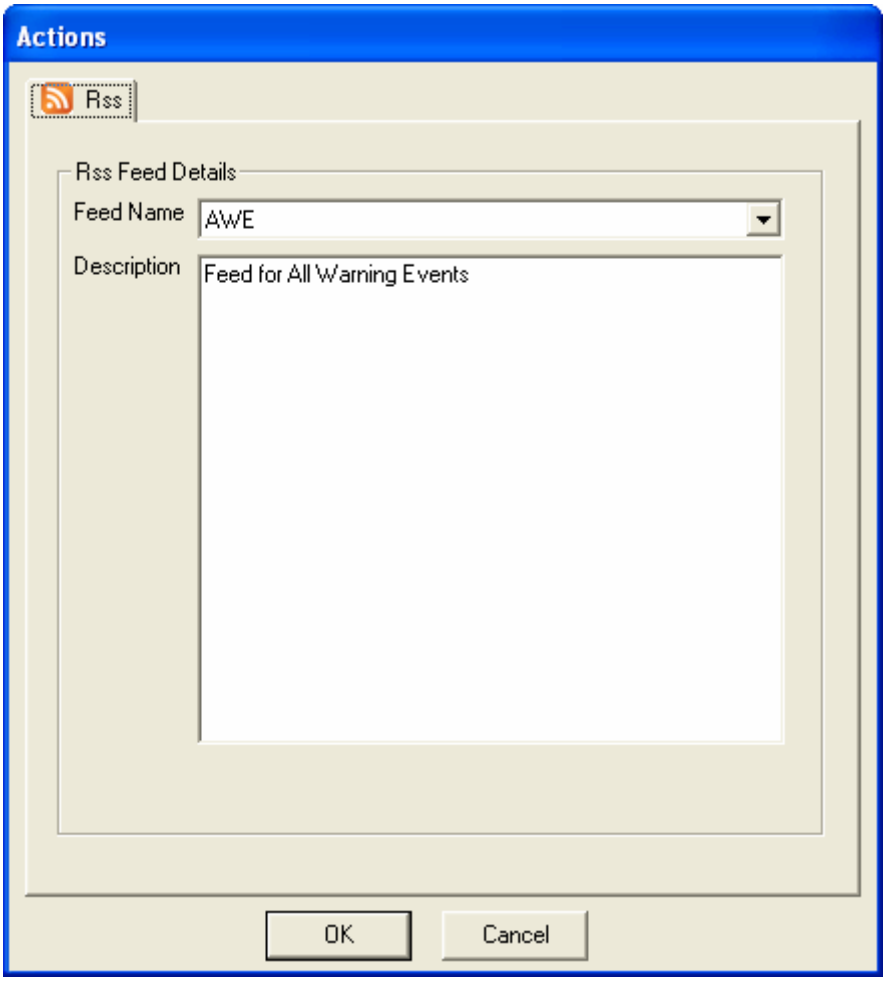
1 Click the **Actions** tab.

EventTracker displays the Actions tab.

2 Select the **Update RSS Feed** check box.

EventTracker displays the Actions-RSS dialog box.

Figure 87 Actions - RSS



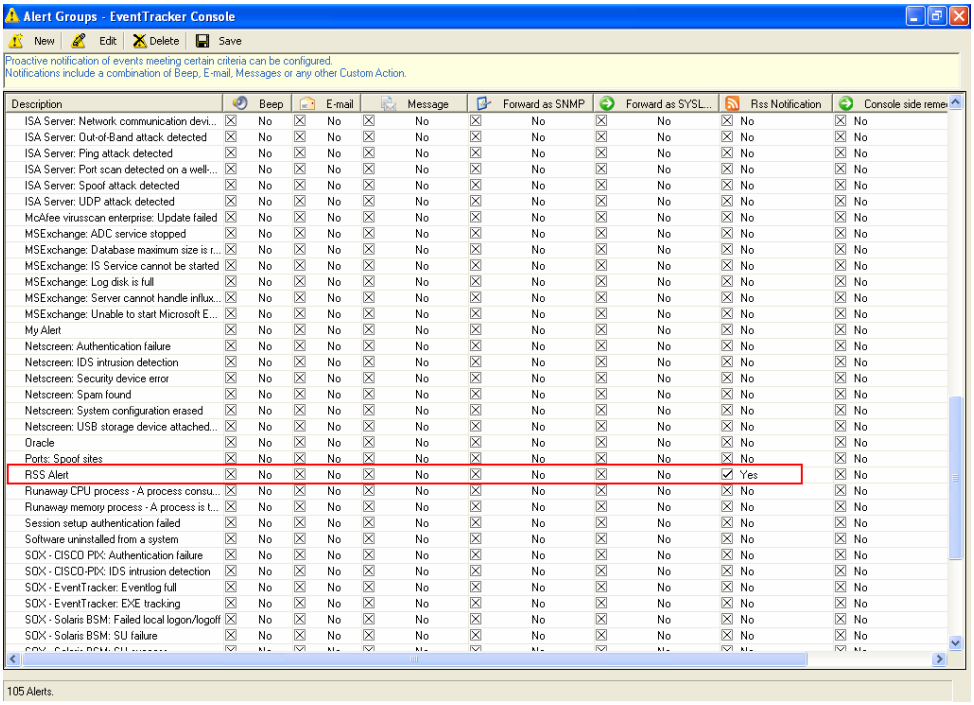
3 Select RSS Feed from the **Feed Name** drop-down list.

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the Alert Groups console with the newly created console message alert.

Figure 88 Alert Groups console


Alert Groups - EventTracker Console
New
Edit
Delete
Save
Proactive notification of events meeting certain criteria can be configured.
Notifications include a combination of Beep, E-mail, Messages or any other Custom Action.
Description
Beep
E-mail
Message
Forward as SNMP
Forward as SYSL...
Rss Notification
Console side rem
ISA Server: Network communication devi...
ISA Server: Out-of-Band attack detected
ISA Server: Ping attack detected
ISA Server: Port scan detected on a well-...
ISA Server: Spoof attack detected
ISA Server: UDP attack detected
McAfee virusscan enterprise: Update failed
MSExchange: ADC service stopped
MSExchange: Database maximum size is r...
MSExchange: IS Service cannot be started
MSExchange: Log disk is full
MSExchange: Server cannot handle influx...
MSExchange: Unable to start Microsoft E...
My Alert
Netscreen: Authentication failure
Netscreen: IDS intrusion detection
Netscreen: Security device error
Netscreen: Spam found
Netscreen: System configuration erased
Netscreen: USB storage device attached...
Oracle
Ports: Spoof sites
RSS Alert
Runaway CPU process - A process consu...
Runaway memory process - A process is t...
Session setup authentication failed
Software uninstalled from a system
SOX - CISCO PIX: Authentication failure
SOX - CISCO-PIX: IDS intrusion detection
SOX - EventTracker: Eventlog full
SOX - EventTracker: EXE tracking
SOX - Solaris BSM: Failed local logon/logoff
SOX - Solaris BSM: SU failure
105 Alerts.

6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Forwarding Events as SNMP Traps

All incoming events are compared with the configured Alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as an SNMP trap to the specified destination.

To forward events as SNMP traps

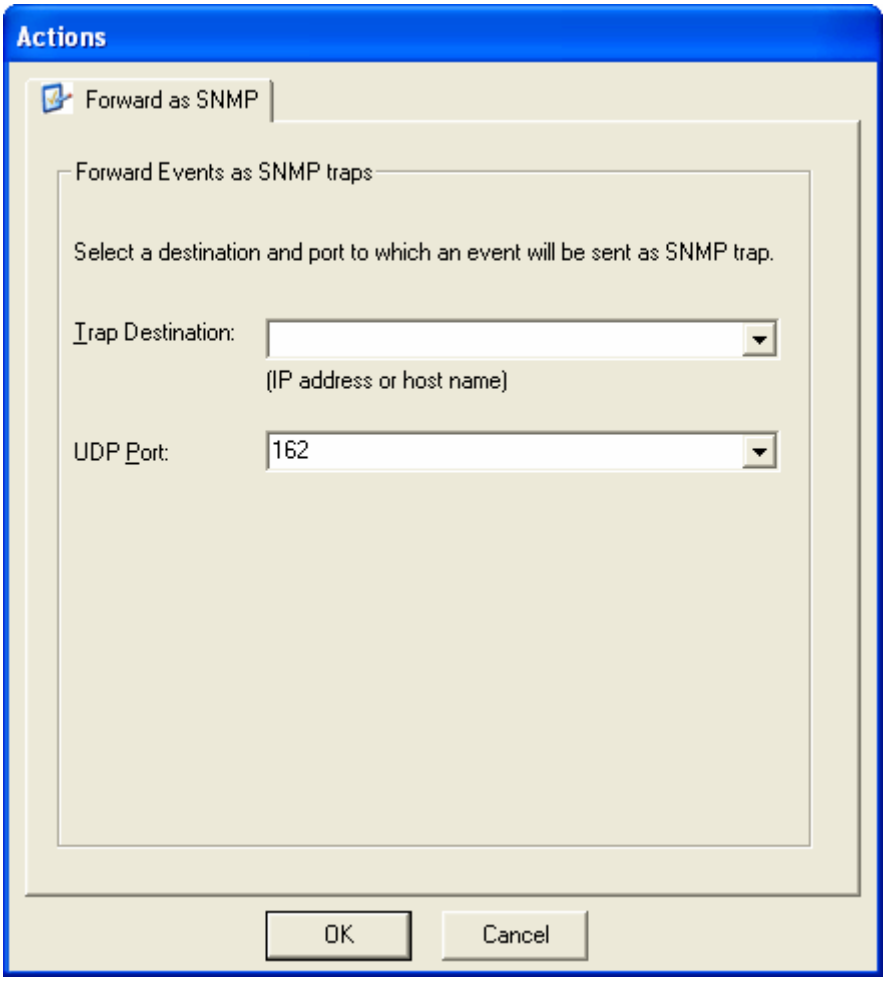
1 Click the **Actions** tab.

EventTracker displays the Actions tab.

2 Select the **Forward Events as SNMP trap** check box.

EventTracker displays the Actions-Forward dialog box.

Figure 89 Actions – Forward as SNMP



Note

You can also access the Actions-Forward dialog box by selecting the corresponding check box under Forward column on the Alerts Group dialog box.

Table 22

Field	Description
Forward Events as SNMP Traps	
Trap Destination	Type the IP address or host name (OR) select a trap destination from the drop-down list.
UDP Port	Type the UDP port number in this field. This field supports numeric data type only.

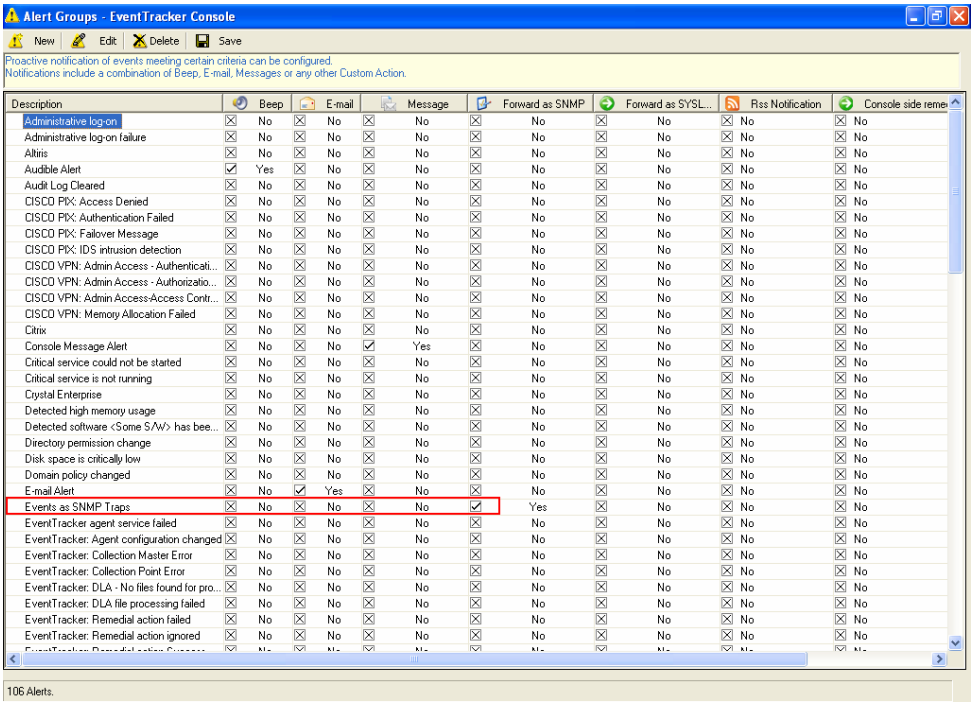
3 Type appropriately in the relevant fields.

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the Alert Groups console with the newly created alert.

Figure 90 Alert Groups console



6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Forwarding Events as SYSLOG Messages

All incoming events are compared with the configured Alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as an SYSLOG message to the specified destination.

To forward events as Syslog messages

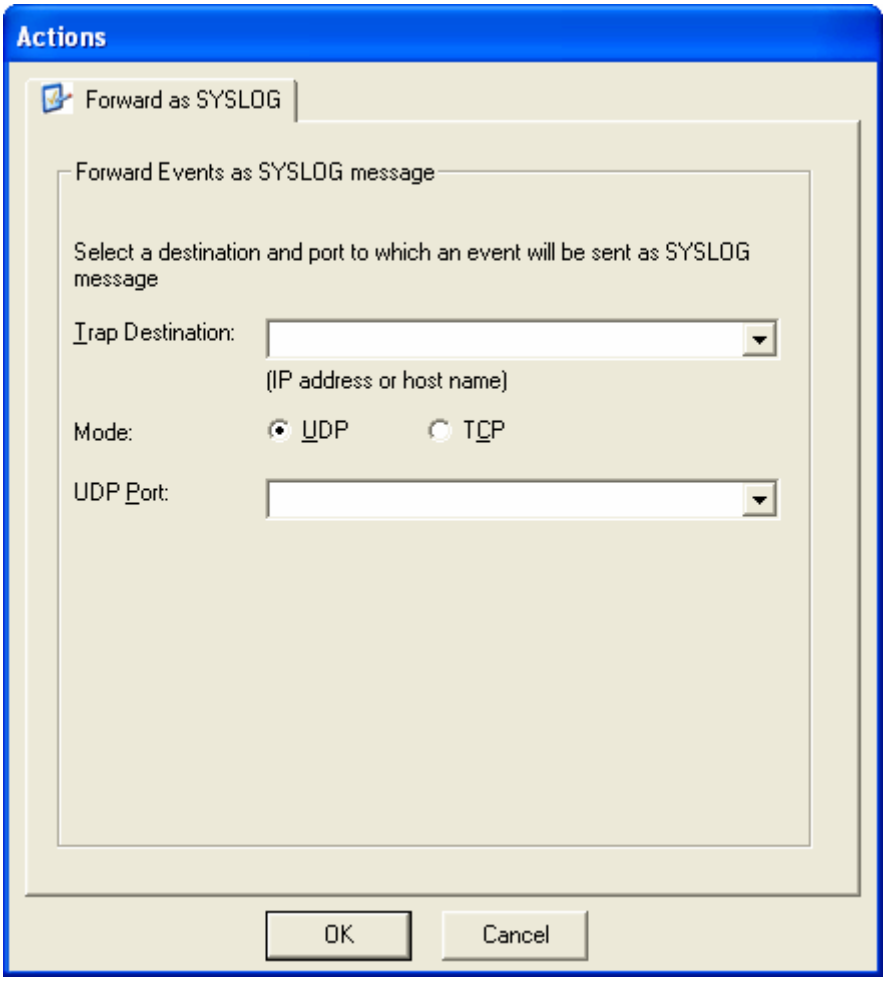
1 Click the **Actions** tab.

EventTracker displays the Actions tab.

2 Select the **Forward Events as SYSLOG message** check box.

EventTracker displays the Actions-Forward dialog box.

Figure 91 Actions - Forward as SYSLOG



Note

You can also access the Actions-Forward dialog box by selecting the corresponding check box under Forward column on the Alerts Group dialog box.

Table 23

Field	Description
Forward Events as SYSLOG messages	
Trap	Type the IP address or host name (OR) select a trap destination

Field	Description
Destination	from the drop-down list.
Mode: Select the transport mode and then select the port corresponding to the mode of transport selected.	

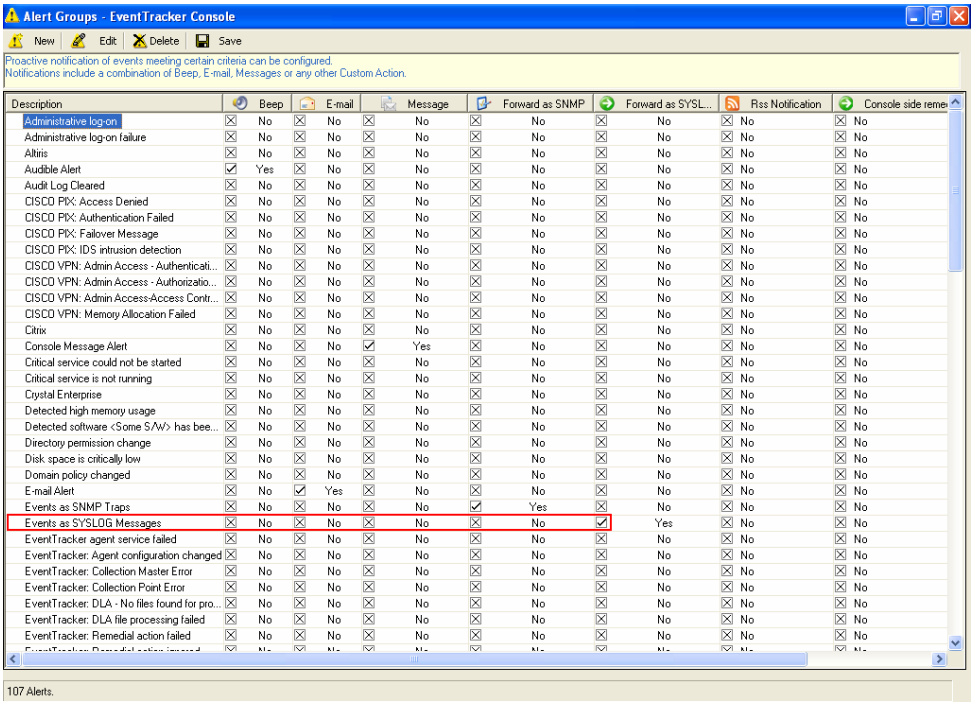
3 Type appropriately in the relevant fields.

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the Alert Groups console with the newly created alert.

Figure 92 Alert Groups console



6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Executing Remedial Action at EventTracker Manager Console System

This option enables you to configure custom action to be executed on receipt of an event at the Manager system.

To execute a custom action

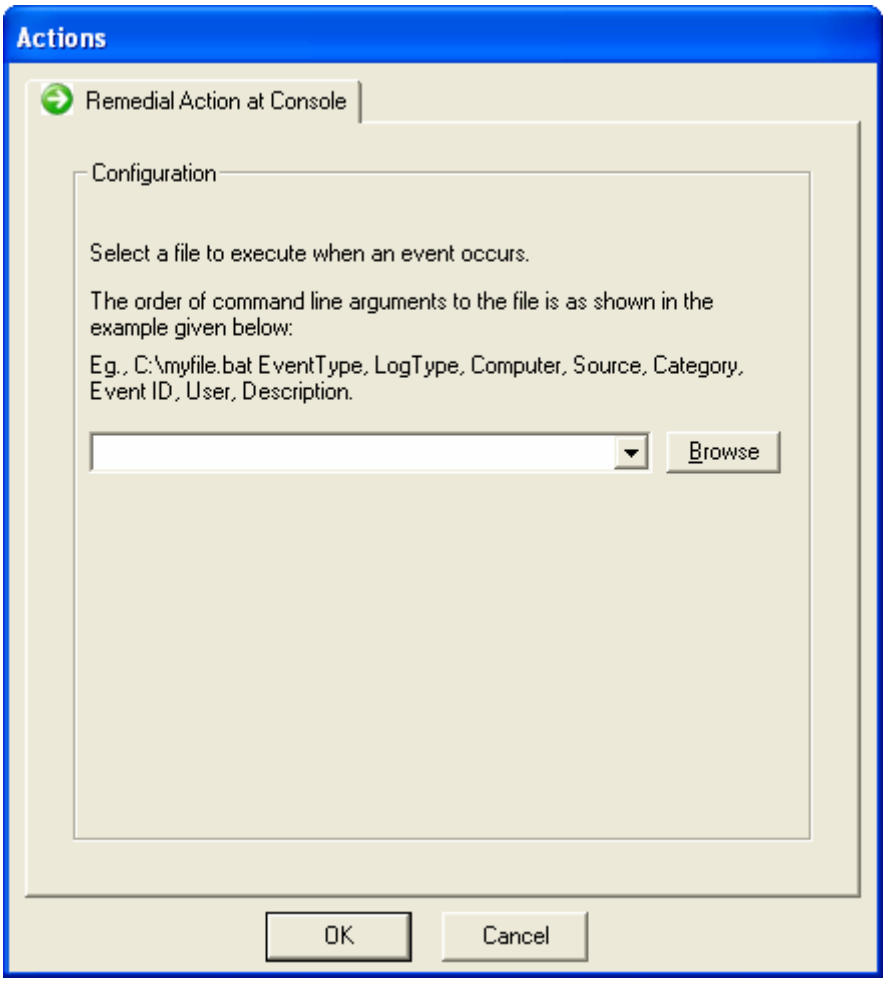
1. Click the **Actions** tab.

   EventTracker displays the Actions tab.

2. Select the **Execute remedial action at EventTracker Console** check box.

   EventTracker displays the Remedial Action at Console dialog box.

Figure 93 Actions – Remedial Action at Console


Actions
Remedial Action at Console
Configuration
Select a file to execute when an event occurs.
The order of command line arguments to the file is as shown in the example given below:
Eg., C:\myfile.bat EventType, LogType, Computer, Source, Category, Event ID, User, Description.
Browse
OK
Cancel

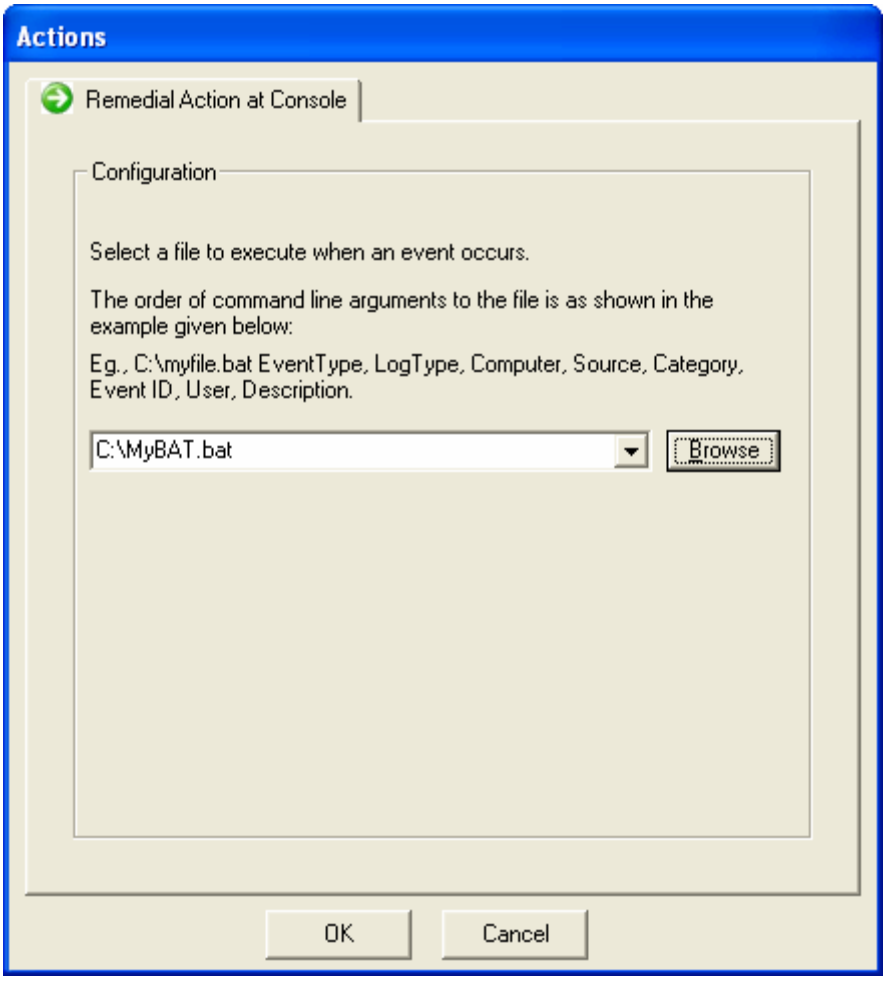
Note

You can also access the Remedial Action at Console dialog box by selecting the corresponding check box under Remedial Action at Console on the Alerts Group dialog box.

3 Click **Browse** under Custom Configuration, navigate and select the appropriate file to execute when an event occurs and then click **OK**.

EventTracker displays the Remedial Action at Console dialog box.

Figure 94 Actions – Remedial Action at Console

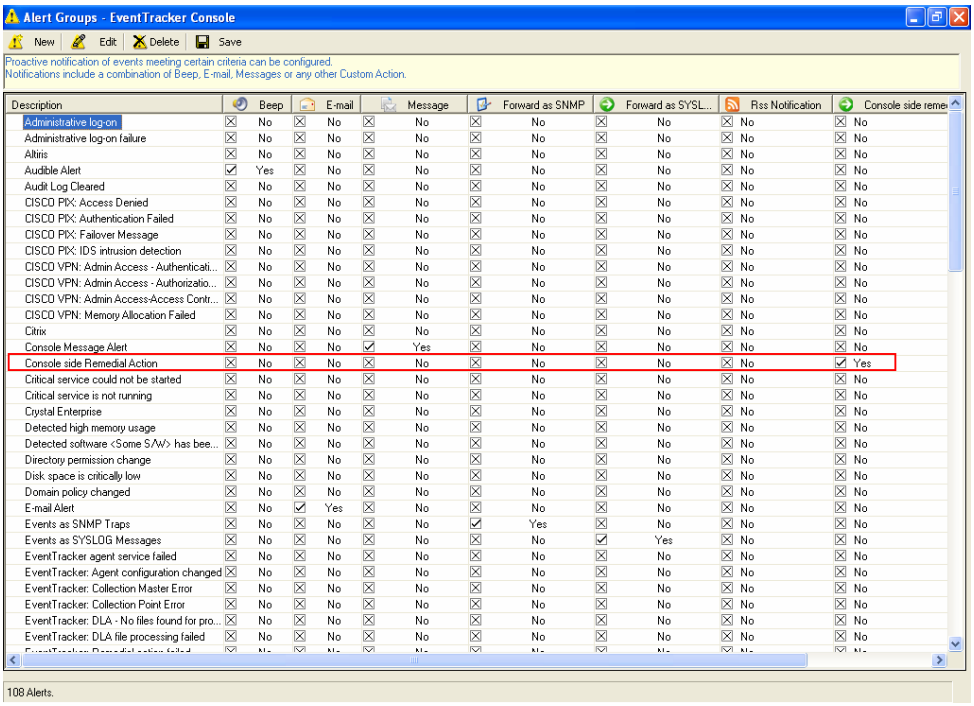

Actions
Remedial Action at Console
Configuration
Select a file to execute when an event occurs.
The order of command line arguments to the file is as shown in the example given below:
Eg., C:\myfile.bat EventType, LogType, Computer, Source, Category, Event ID, User, Description.
C:\MyBAT.bat
Browse
OK
Cancel

4 Click **OK**.

5 Click **OK** on the Alert Group Configuration dialog box.

EventTracker displays the Alert Groups console with the newly created custom action alert.

Figure 95 Alert Groups console



6 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

7 Click **OK**.

8 Restart the Management Console.

Editing Alert Actions

This option enables you to edit Alert actions.

To edit Alert actions

1 Select the Alert for which you want to modify the action in the Alert Groups – EventTracker Console.

2 Click **Edit**.

(OR)

Double-click the Alert.

EventTracker displays the Alert Group Configuration – EventTracker Console.

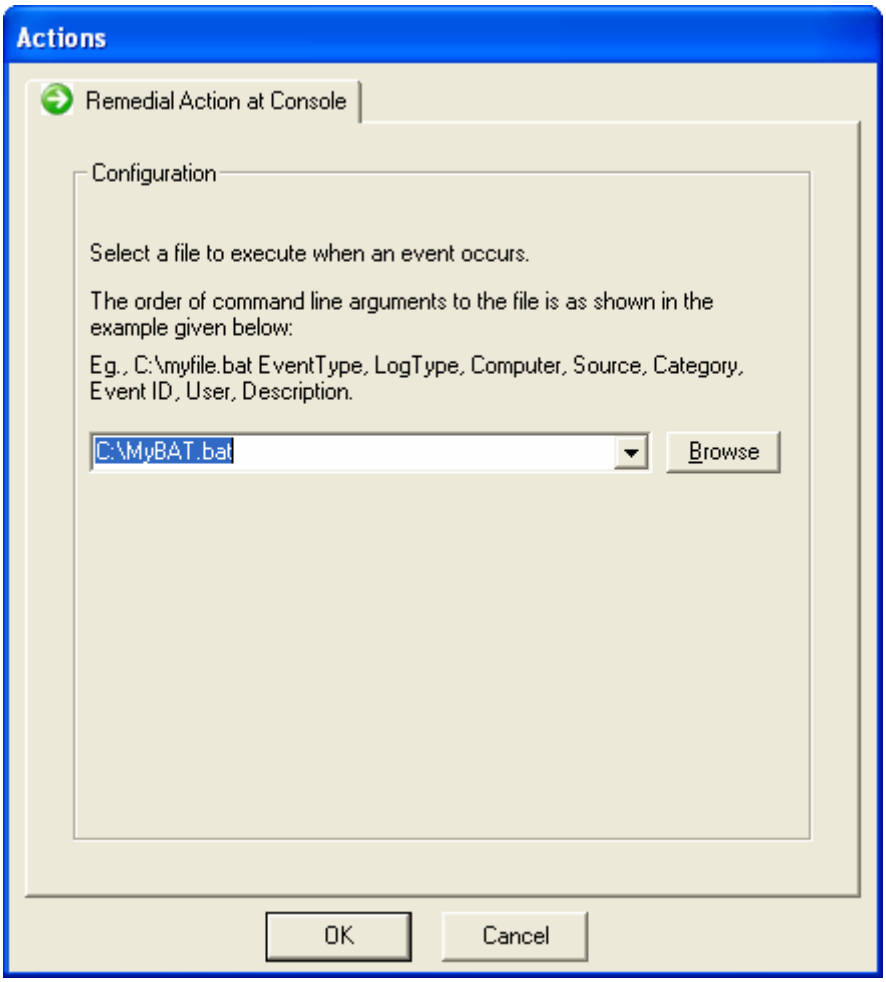
3 Click the **Actions** tab.

EventTracker displays the Actions tab.

4 Click **Edit Actions**.

EventTracker displays the Actions dialog box.

Figure 96 Editing Actions


Actions
Remedial Action at Console
Configuration
Select a file to execute when an event occurs.
The order of command line arguments to the file is as shown in the example given below:
Eg., C:\myfile.bat EventType, LogType, Computer, Source, Category, Event ID, User, Description.
C:\MyBAT.bat
Browse
OK
Cancel

5 Click **Browse**.

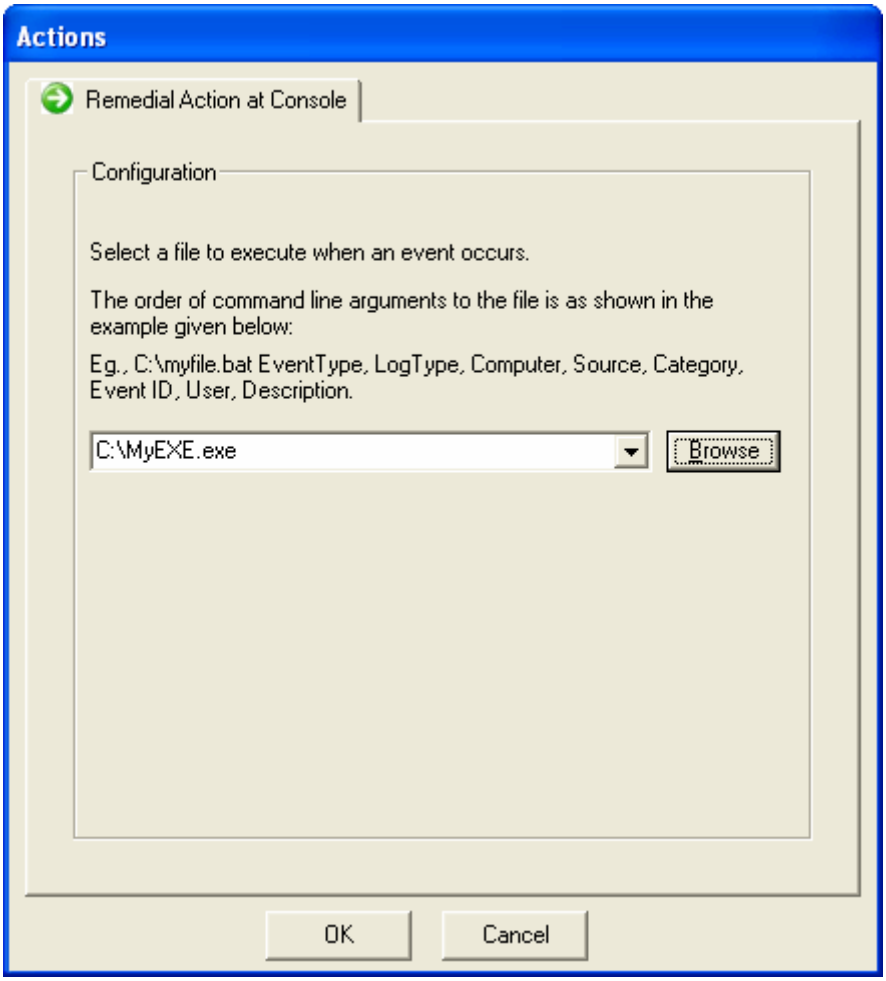
EventTracker displays the Open dialog box.

6 Go to the appropriate folder and select the file to be executed.

7 Click **Open**.

EventTracker displays the Actions dialog box.

Figure 97 Editing Actions


Actions
Remedial Action at Console
Configuration
Select a file to execute when an event occurs.
The order of command line arguments to the file is as shown in the example given below:
Eg., C:\myfile.bat EventType, LogType, Computer, Source, Category, Event ID, User, Description.
C:\MyEXE.exe
Browse
OK
Cancel

8 Click **OK** on the Actions dialog box.

9 Click **Finish** on the Alert Group Configuration – EventTracker Console dialog box.

10 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

11 Click **OK**.

12 Restart the Management Console.

Executing Remedial Action at EventTracker Agent System

Upon receiving Events that fall under Alerts Category, EventTracker can be configured to

- Raise a beep sound from the PC speaker
- Send e-mail to one or more recipients
- Send network message to specific devices are connected to the network
- Forward events as Traps to specific devices
- Console side remedial action

All these actions are performed at the system where EventTracker Manager is installed.

Agent side remedial action helps to perform remedial actions at the system where EventTracker Agent is installed.

Note

You cannot execute remedial actions at non-Windows and Agentless systems.

To execute remedial action

1. Click the **Actions** tab.

   EventTracker displays the Actions tab.

2. Select the **Execute remedial action at EventTracker Agent** check box.

   EventTracker displays the Remedial Action at Agent dialog box.

Figure 98 Actions – Remedial Action at Agent

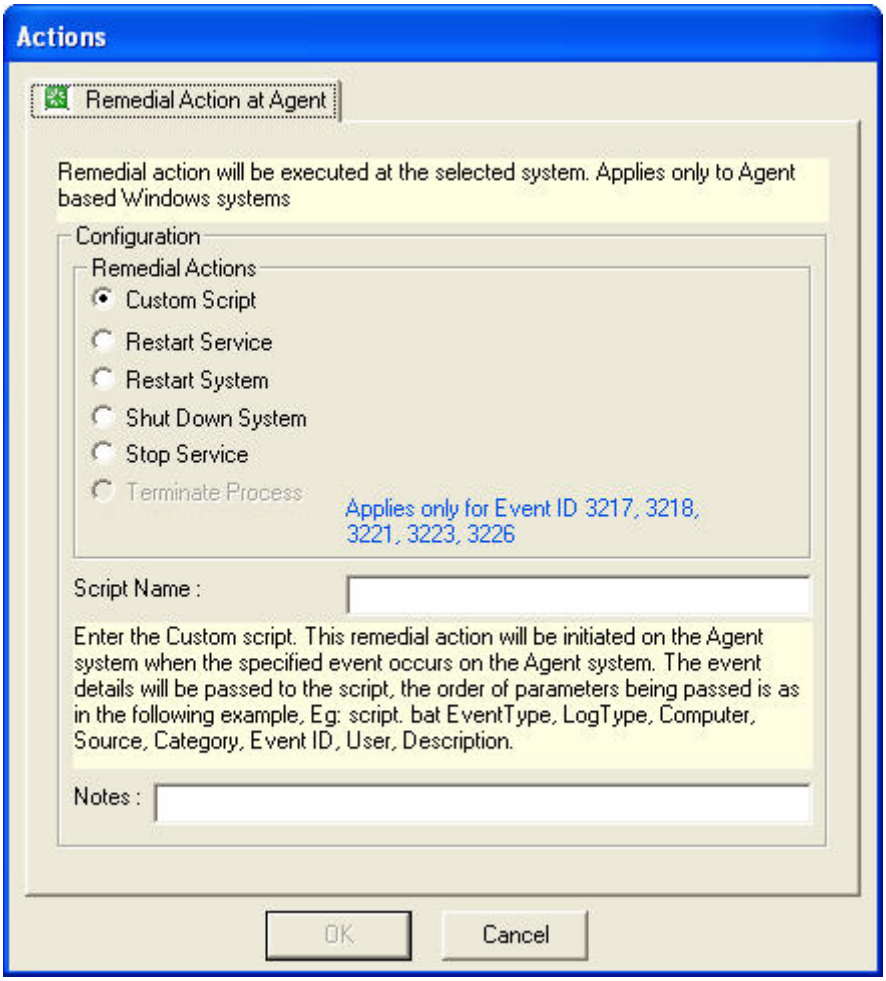

Actions
Remedial Action at Agent
Remedial action will be executed at the selected system. Applies only to Agent based Windows systems
Configuration
Remedial Actions
Custom Script
Restart Service
Restart System
Shut Down System
Stop Service
Terminate Process
Applies only for Event ID 3217, 3218, 3221, 3223, 3226
Script Name :
Enter the Custom script. This remedial action will be initiated on the Agent system when the specified event occurs on the Agent system. The event details will be passed to the script, the order of parameters being passed is as in the following example, Eg: script. bat EventType, LogType, Computer, Source, Category, Event ID, User, Description.
Notes :
OK
Cancel

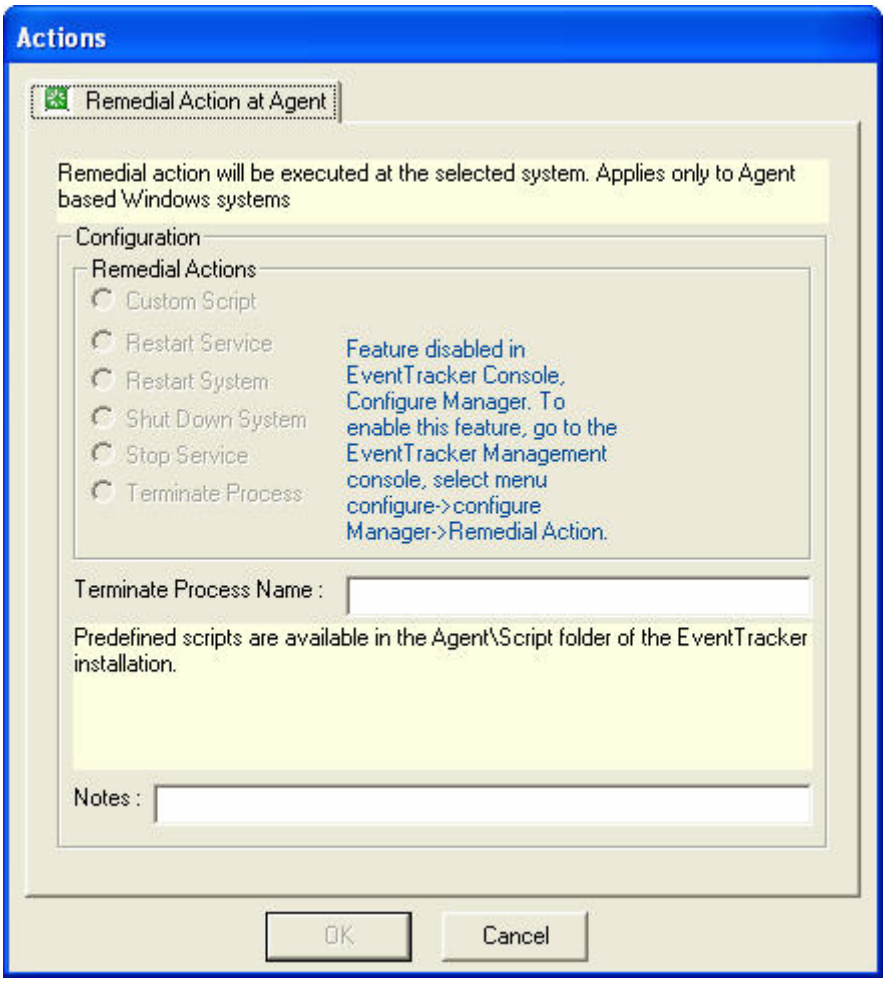
Table 24

Field	Description
Custom Script	Type the name of the script in **Script Name** field. Script files are stored in the default EventTracker Agent installation path typically …\Program Files\Prism Microsystems\EventTracker\Agent Type appropriate description in the **Notes** field for future reference.
Restart Service	Type the name of the service that you want to restart in **Service Name** field. Type appropriate description in the **Notes** field for future reference.
Restart System	EventTracker disables the **Script Name** field. Type appropriate description in the **Notes** field for future reference.
Shut Down System	EventTracker disables the **Script Name** field. Type appropriate description in the **Notes** field for future reference.
Stop Service	Type the name of the service that you want to stop in **Service Name** field. Type appropriate description in the **Notes** field for

Field	Description
	future reference.
Terminate Process	EventTracker enables this option only when you set an alert for the specified Events.

As said earlier you ought to enable Remedial Action in the Manager Configuration window. Had you not enabled, EventTracker will display Actions window with appropriate message to enable Remedial Action.

Figure 99 Actions - Remedial Action at Agent


Actions
Remedial Action at Agent
Remedial action will be executed at the selected system. Applies only to Agent based Windows systems
Configuration
Remedial Actions
Custom Script
Restart Service
Restart System
Shut Down System
Stop Service
Terminate Process
Feature disabled in EventTracker Console, Configure Manager. To enable this feature, go to the EventTracker Management console, select menu configure->configure Manager->Remedial Action.
Terminate Process Name :
Predefined scripts are available in the Agent\Script folder of the EventTracker installation.
Notes :
OK
Cancel

3 Select an appropriate option and then click **OK**.

EventTracker displays the Alert Groups console with the newly created custom action alert.

4 Click **Save** on the toolbar.

EventTracker displays the EventTracker Management Console Message.

5 Click **OK**.

6 Restart the Management Console.

Configuring Alert Actions for predefined Alerts

To configure alert actions for predefined Alerts

1 Open the Alert Groups console.

2 Double-click the predefined Alert for which you want to set notification.

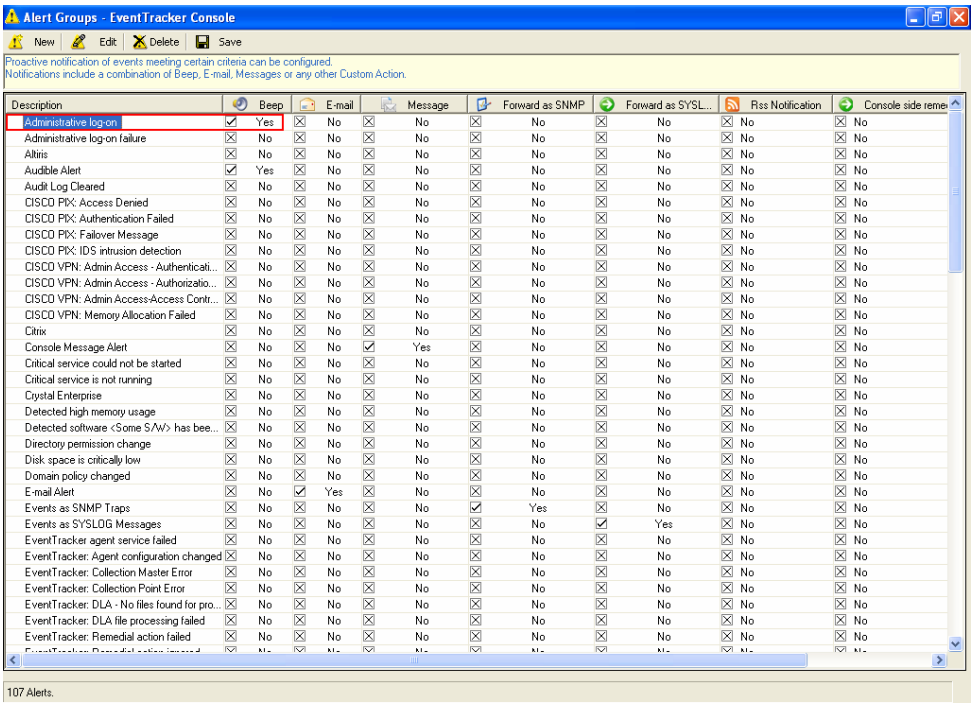
> **Note**
>
> By default, predefined Alerts are applicable for all monitored systems.

3 Select the appropriate check boxes.

4 Configure the settings appropriately.

EventTracker displays the Alert Groups console.

Figure 100 Alert Groups console



5 Click **Save** to save the settings.

Note

In this example, the Administrative log-on Alert has been selected and configured to Beep whenever the Administrator or a user with Administrator's privilege logs in to your system. Note the tick mark in the Beep column. To remove the settings, just click on the tick mark.

Adding Alerts from the Dashboard

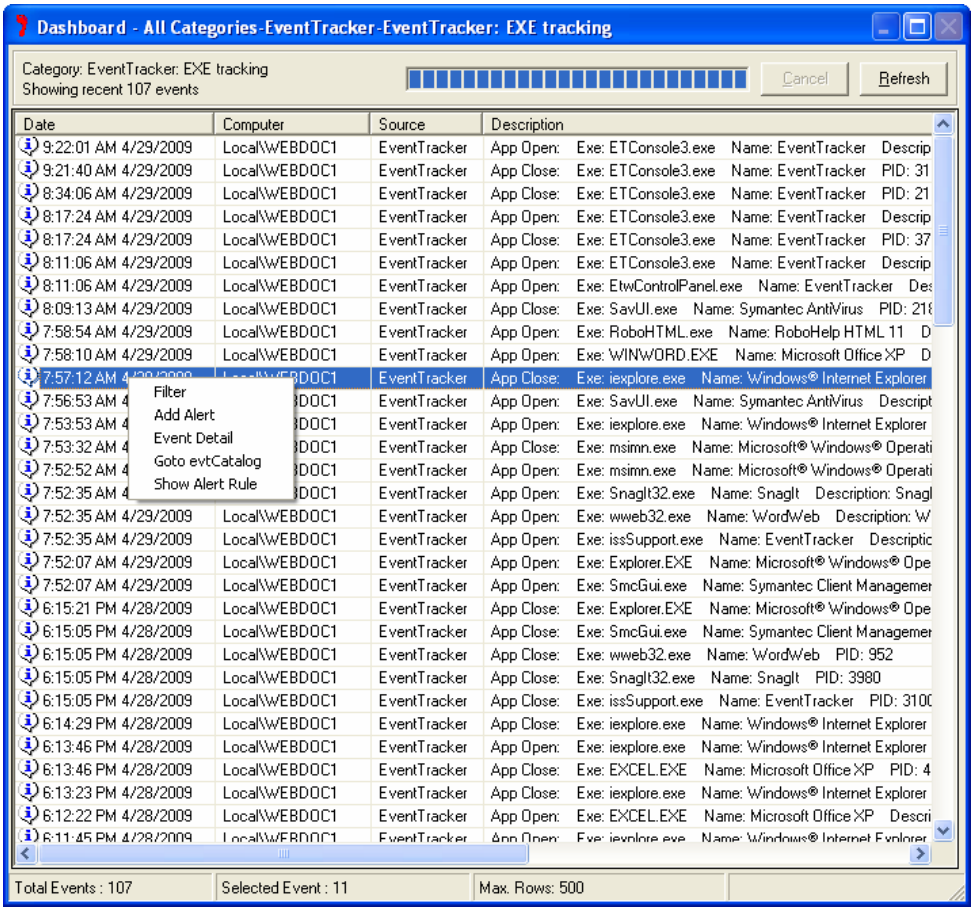
This option helps you access the Alert Group Configuration console from the Dashboard

To add Alerts from the Dashboard

- Right-click the event that you want to configure as alert.

  EventTracker displays the shortcut menu.

Figure 101
Management Console
– Shortcut menu



From the shortcut menu, choose the **Add Alert** option.

EventTracker displays the **Alert Name** tab on the Alert Group Configuration console.

Chapter 5
Configuring RSS Feeds

In this chapter, you will learn how to:

- Cofigure RSS Feeds

RSS Feeds

RSS/XML feeds can send notification to your computer upon generation of Advanced reports or Alerts raised by EventTracker. Contents will fly to your desktop faster than an e-mail notification.

EventTracker does not delete a RSS Feed permanently, when you delete it, rather it does make it inactive.

Adding RSS feeds

This option helps you add RSS feeds.

To add RSS feeds

1. Open the Management Console.
2. Click the **Configure** menu and select the **RSS Feeds** option.

   EventTracker displays the RSS Feeds window.

Figure 102 RSS Feeds

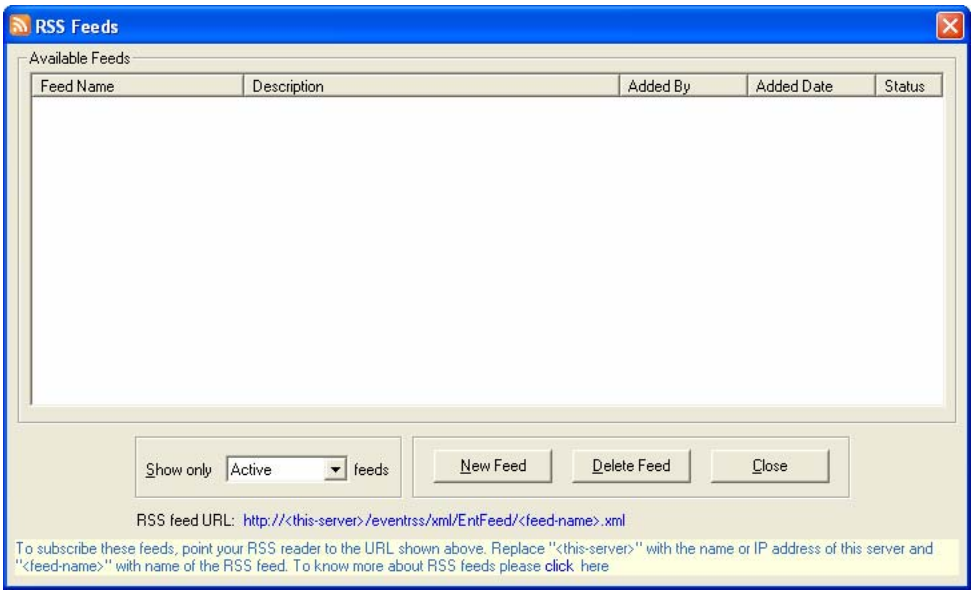


Table 25

Field	Description
Available Feeds	
Feed Name	Displays the name of the feed.
Description	Displays the description of the feed.
Added By	Displays the name of the user who configured the feed.

Field	Description
Added Date	Displays the date when the feed was added.
Status	Displays whether the RSS Feeds are active or inactive.
Show only	Select from the drop-down list to view **All**, **Active** and **Inactive** feeds.

Table 26

Click	To
New Feed	Add new feeds.
Delete Feed	Delete feeds. Once the feeds are deleted, they are not deleted from the db permanently; rather EventTracker changes the status of the feeds as **Inactive**. Inactive feeds cannot be reactivated.
Close	Close RSS Feeds window.

3 Click **New Feed**.

EventTracker displays the New RSS Feed window.

Figure 103 New RSS Feed

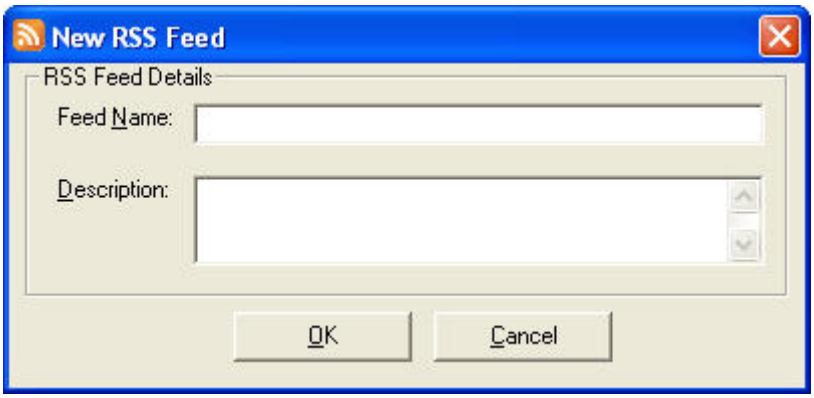
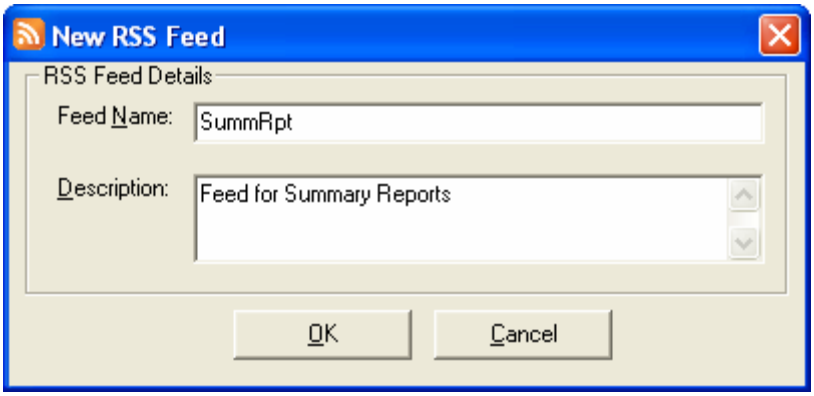


Table 27

Field	Description
RSS Feed Details	
Feed Name	Type the name of the feed.
Description	Type the description of the feed.

4 Type appropriately in the relevant fields.

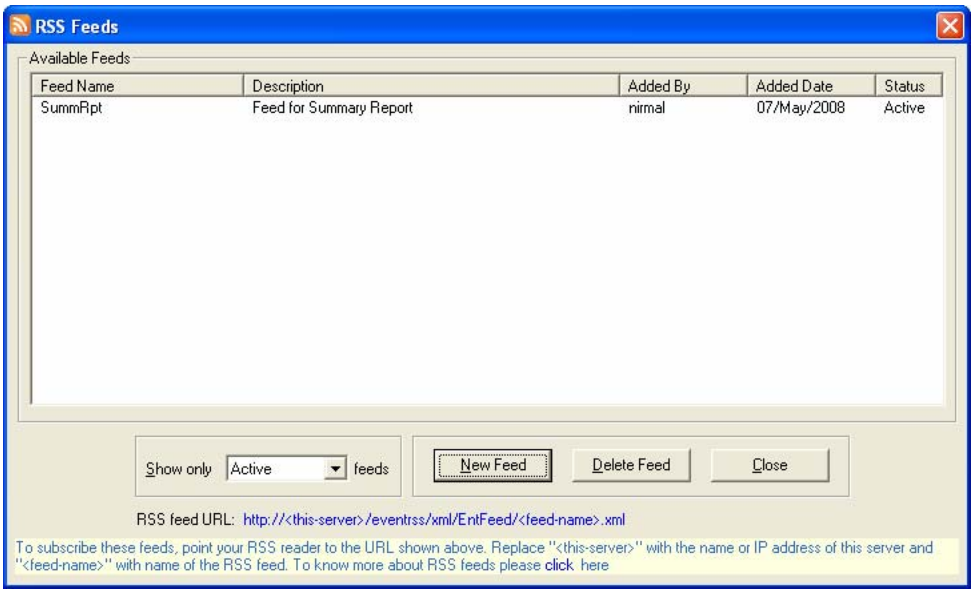
Figure 104 New RSS Feed



5 Click **OK**.

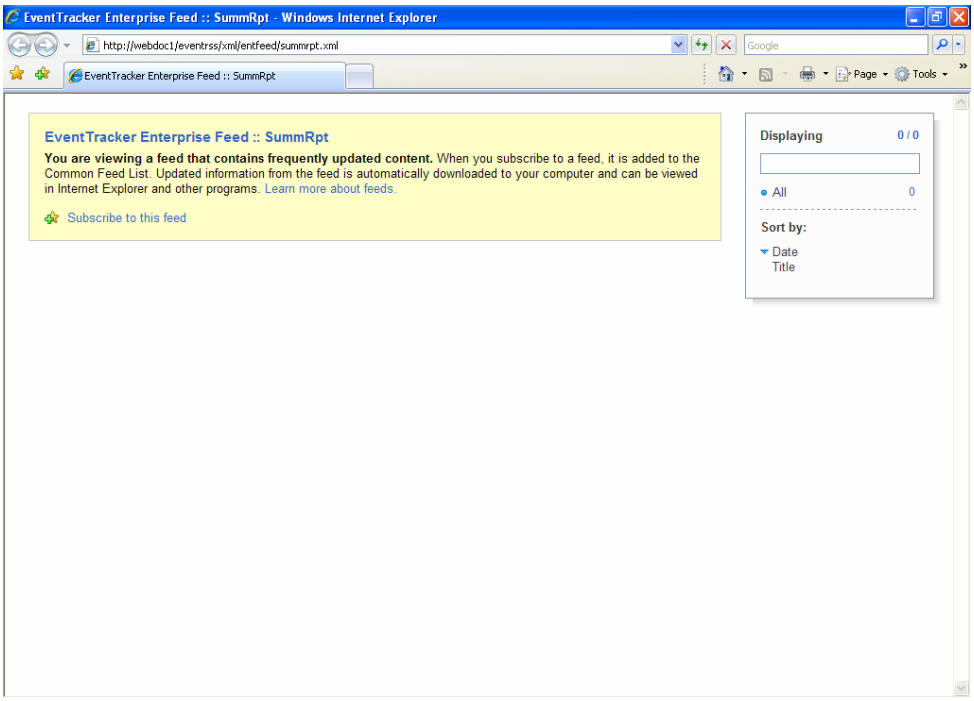
EventTracker displays the RSS Feeds window with newly added RSS feed.

Figure 105 RSS Feeds



6 Type the URL in the address bar of the browser as advised on the RSS Feeds window.

Figure 106 RSS Feeds Web page


EventTracker Enterprise Feed :: SummRpt - Windows Internet Explorer
http://webdoc1/eventrss/xml/entfeed/summrpt.xml
EventTracker Enterprise Feed :: SummRpt
EventTracker Enterprise Feed :: SummRpt
You are viewing a feed that contains frequently updated content. When you subscribe to a feed, it is added to the Common Feed List. Updated information from the feed is automatically downloaded to your computer and can be viewed in Internet Explorer and other programs. Learn more about feeds.
Subscribe to this feed
Displaying 0 / 0
All 0
Sort by:
Date
Title

Note

You need to have IE v7.0 and above to subscribe to RSS Feeds. You can also add the feed links to RSS Reader.

7 Click **Close** on the RSS Feeds window.

Deleting RSS Feeds

This option helps you delete RSS feeds.

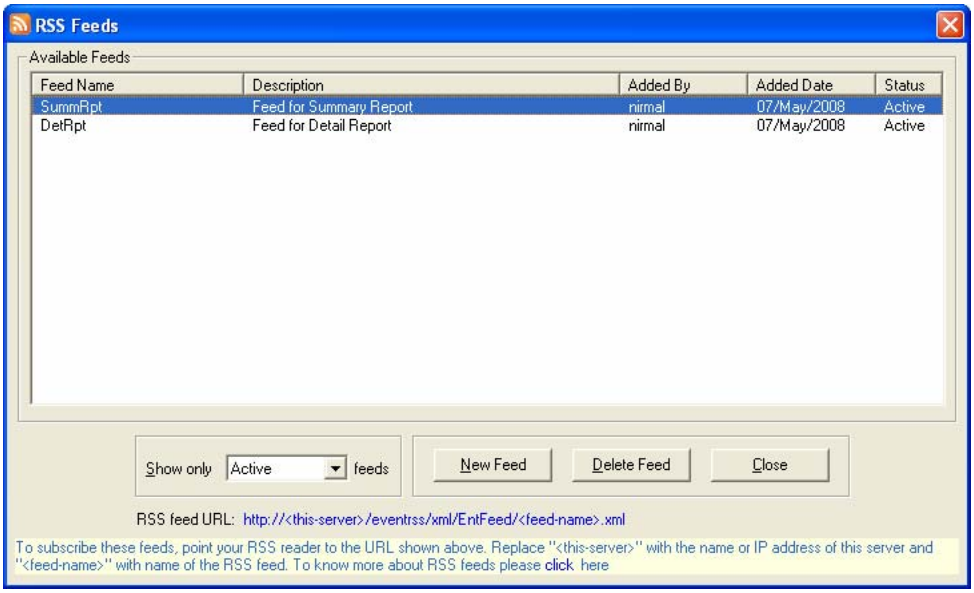
To delete RSS feeds

1 Open the Management Console.

2 Click the **Configure** menu and select the **RSS Feeds** option.

EventTracker displays the RSS Feeds window.

Figure 107 RSS Feeds

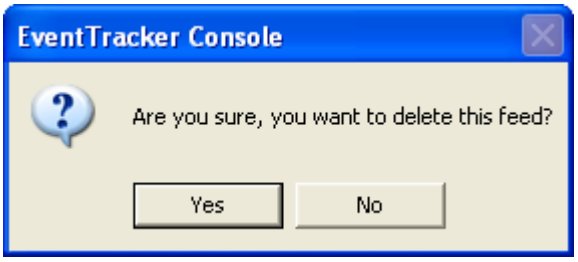


3 Select the Feed that you want to delete from the pool.

4 Click **Delete Feed**.

EventTracker displays the EventTracker Reports Console message box.

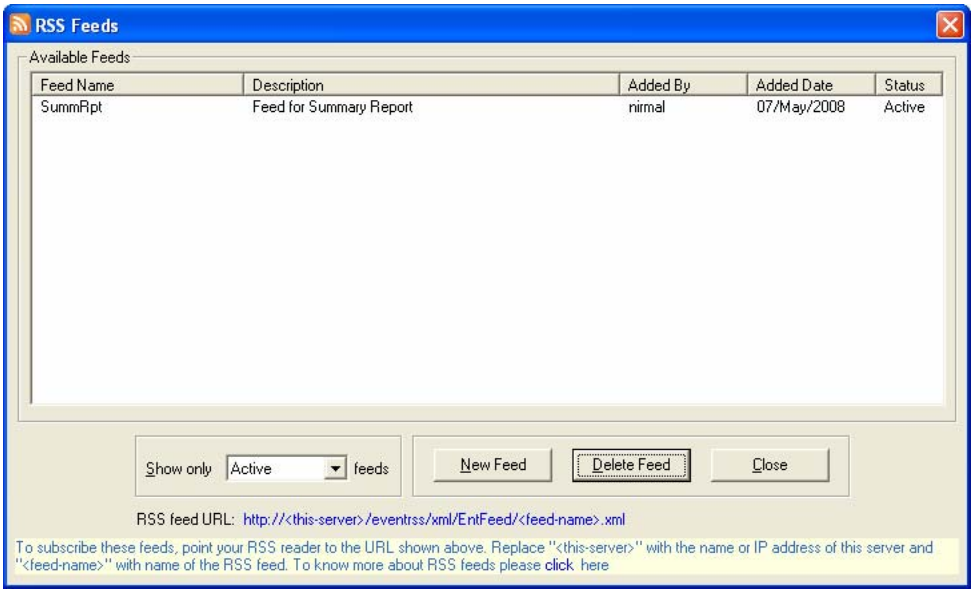
Figure 108 EventTracker Console – message box



5 Click **Yes**.

EventTracker deletes the selected RSS feed.

Figure 109 RSS Feeds

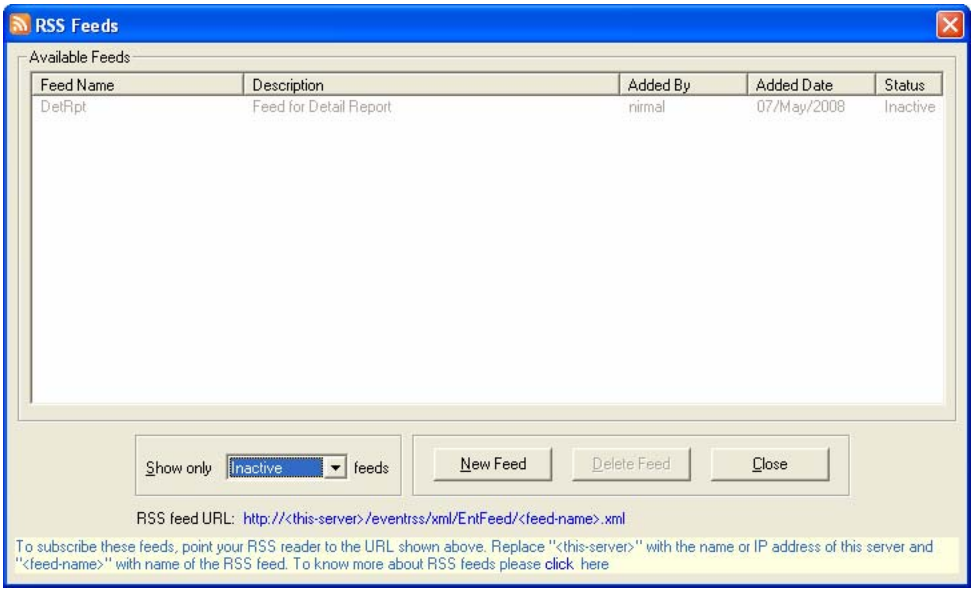


6 To view the deleted feeds, select **Inactive** from the **Show only** drop-down list.

7 To view all Active and Inactive feeds, select **All** from the **Show only** drop-down list.

EventTracker displays the RSS Feeds window.

Figure 110 RSS Feeds



8 Click **Close**.

Chapter 6
Maintenance Tools

In this chapter, you will learn how to:

- Create an Index for Archive Files
- Compact the Database Size

Creating Index for Archive Files

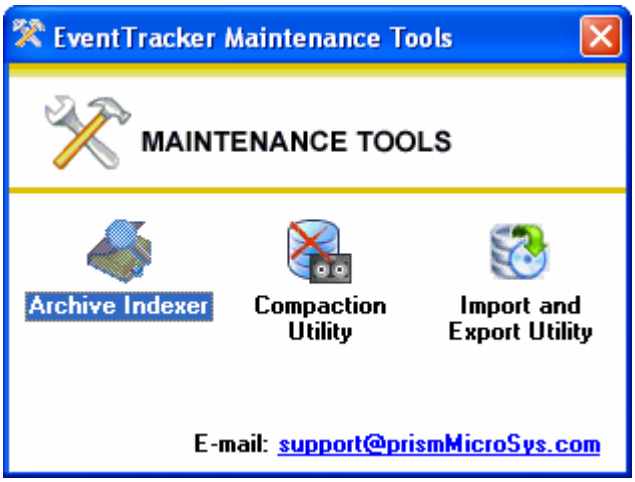
This option enables you to create index for `.cab` files.

To create index for the archive files

1 Double-click **Maintenance Tools** on the EventTracker Control Panel.

EventTracker displays the EventTracker Maintenance Tools window.

Figure 111 Maintenance Tools - splash screen



2 Double-click **Archive Indexer**.

EventTracker displays the Archive Indexer dialog box.

Figure 112 Archive Indexer

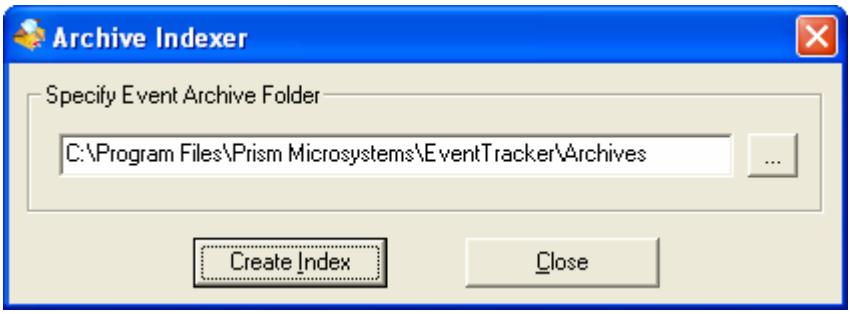


Table 28

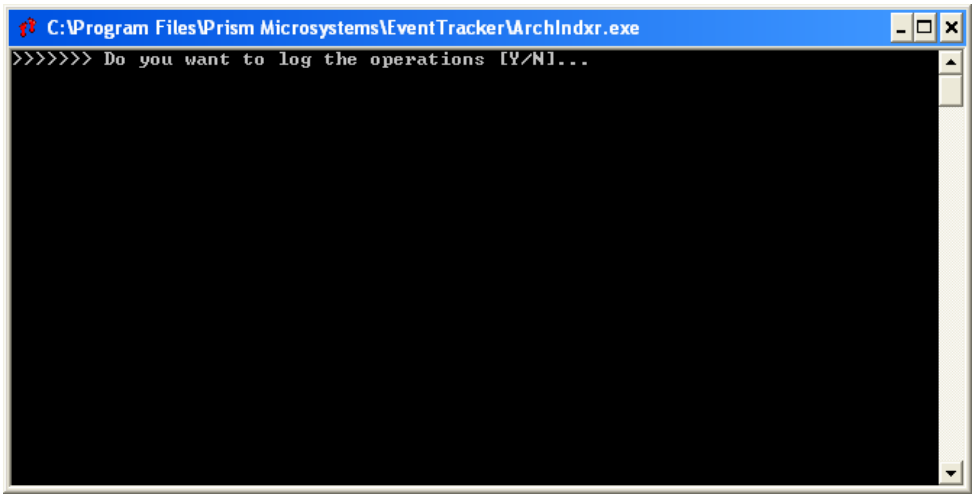
Field	Description
Specify Event Archive Folder	By default, EventTracker displays the path in this field. To change the path, click ..., navigate, and select the folder where the archive files are stored.

3 Type the archive folder path in the **Specify Event Archive Folder** field.

4 Click **Create Index**.

EventTracker displays the DOS window.

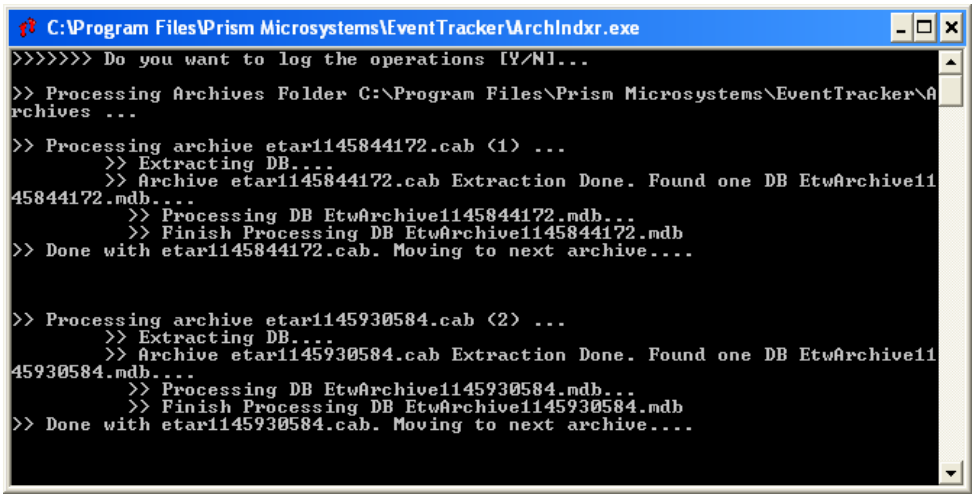
Figure 113 Archive Index – command prompt



5 To have log file, click **Y**. If you do not want to have a log file, click **N**.

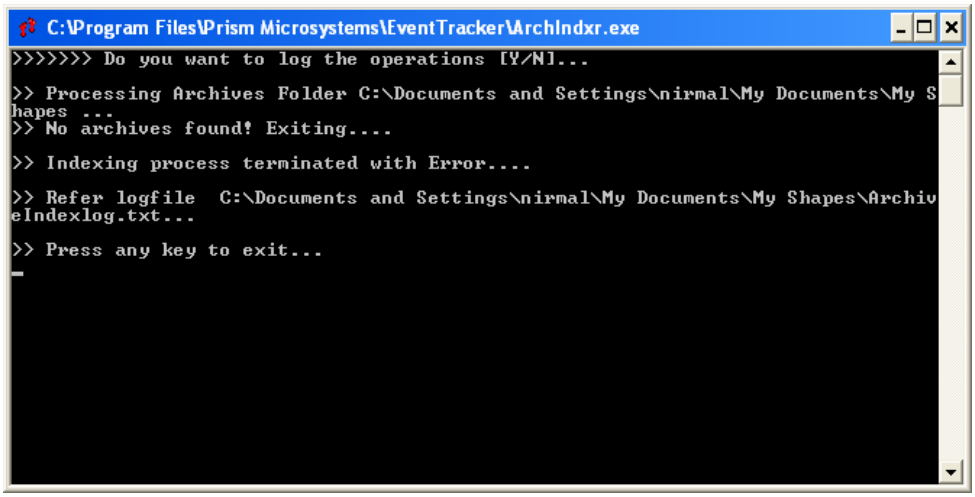
EventTracker starts indexing the archive files and displays the DOS window.

Figure 114 Archive Index – command prompt


C:\Program Files\Prism Microsystems\EventTracker\ArchIndxr.exe
>>>>>>> Do you want to log the operations [Y/N]...
>> Processing Archives Folder C:\Program Files\Prism Microsystems\EventTracker\A
rchives ...
>> Processing archive etar1145844172.cab (1) ...
>> Extracting DB....
>> Archive etar1145844172.cab Extraction Done. Found one DB EtwArchive11
45844172.mdb....
>> Processing DB EtwArchive1145844172.mdb...
>> Finish Processing DB EtwArchive1145844172.mdb
>> Done with etar1145844172.cab. Moving to next archive....
>> Processing archive etar1145930584.cab (2) ...
>> Extracting DB....
>> Archive etar1145930584.cab Extraction Done. Found one DB EtwArchive11
45930584.mdb....
>> Processing DB EtwArchive1145930584.mdb...
>> Finish Processing DB EtwArchive1145930584.mdb
>> Done with etar1145930584.cab. Moving to next archive....

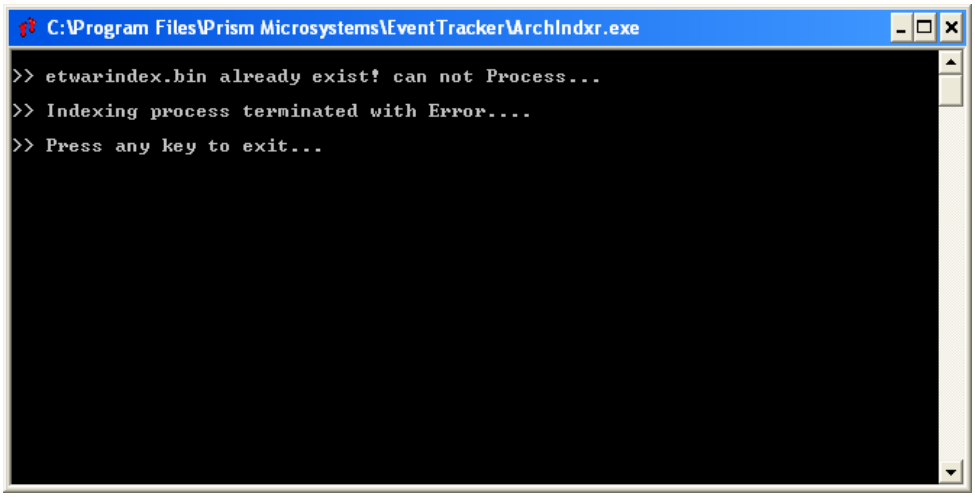
If there are no `.cab` files in the selected folder, EventTracker displays the DOS window.

Figure 115 Archive Index – command prompt


C:\Program Files\Prism Microsystems\EventTracker\ArchIndxr.exe
>>>>>>> Do you want to log the operations [Y/N]...
>> Processing Archives Folder C:\Documents and Settings\nirmal\My Documents\My Shapes ...
>> No archives found! Exiting....
>> Indexing process terminated with Error....
>> Refer logfile C:\Documents and Settings\nirmal\My Documents\My Shapes\ArchiveIndexlog.txt...
>> Press any key to exit...

If an index already exists in the selected folder, EventTracker displays the DOS window.

Figure 116 Archive Index – command prompt


C:\Program Files\Prism Microsystems\EventTracker\ArchIndxr.exe
>> etwarindex.bin already exist! can not Process...
>> Indexing process terminated with Error....
>> Press any key to exit...

Compacting the Database size

This option enables you to compact the database size.

To compact the database size

1. Double-click **Maintenance Tools** on the EventTracker Control Panel.

   EventTracker displays the Maintenance Tools splash screen.

2. Double-click **Compaction Utility**.

EventTracker displays the Compact Files dialog box.

Figure 117 Compact Files – Collection Master Console

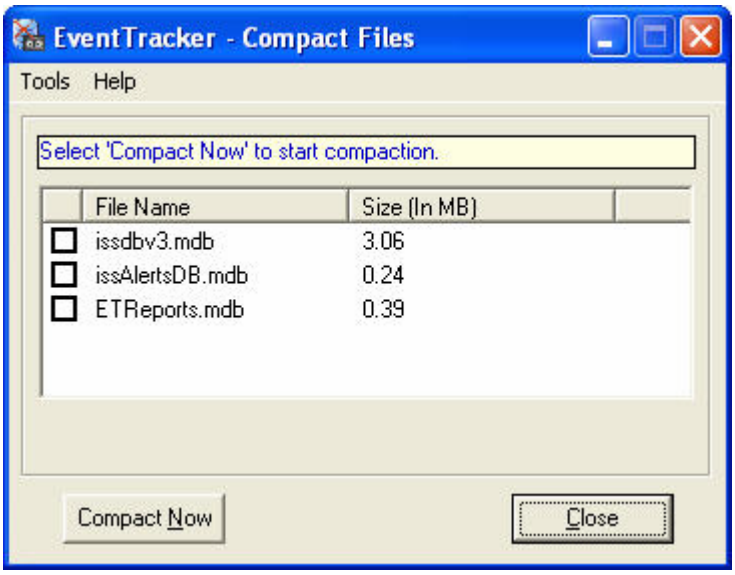


Figure 118 Compact Files – Collection Point Console

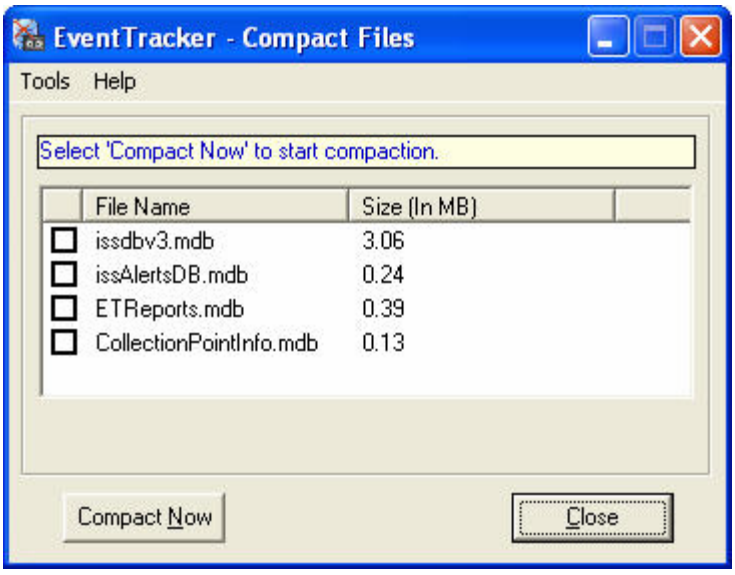


Figure 119 Compact Files – Standard Console

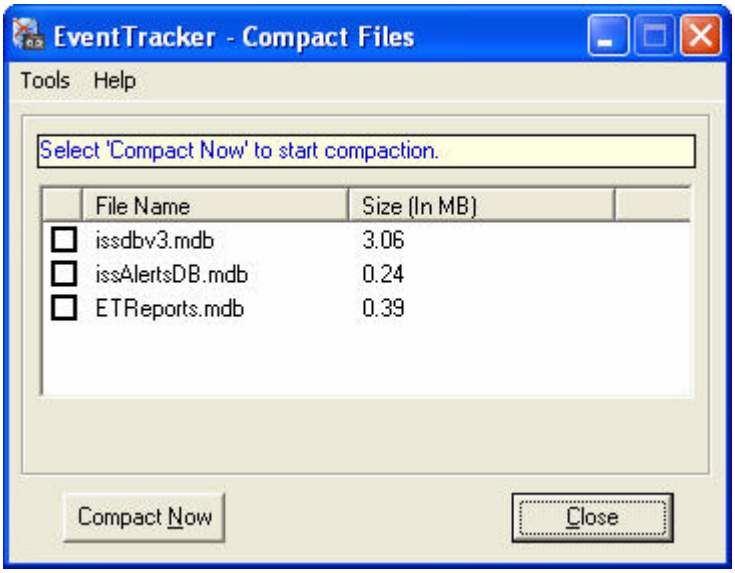


Table 29

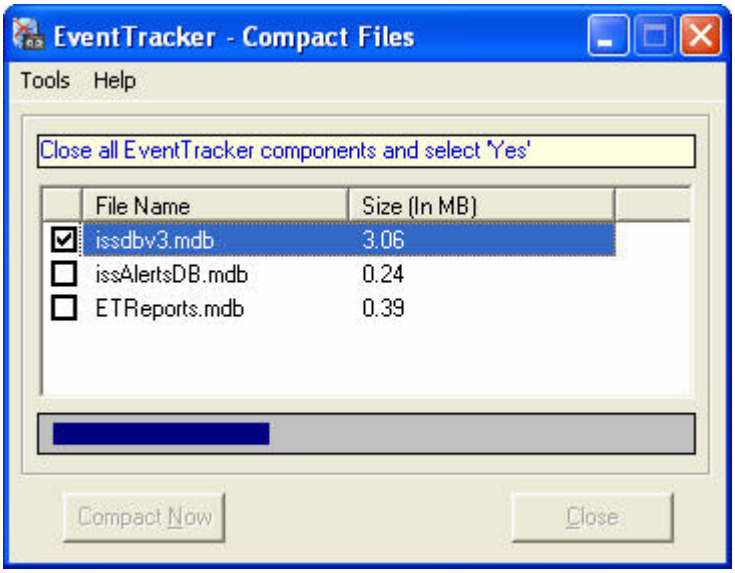
Field	Description
Database Name	Displays the name of the databases.
Database Size (in MB)	Displays the size of the respective databases.

3 Select the check boxes against the databases that you want to compact.

4 Click **Compact Now**.

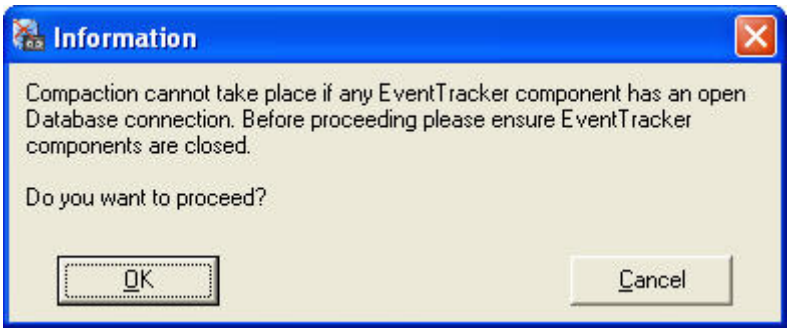
EventTracker starts compacting the database and displays the EventTracker – Compact Database progress bar.

Figure 120 Compact Files – Progress bar



If any EventTracker component has an open Database connection, EventTracker displays the Information message box.

Figure 121 Information – message box


Information
Compaction cannot take place if any EventTracker component has an open Database connection. Before proceeding please ensure EventTracker components are closed.
Do you want to proceed?
OK
Cancel

5 If there is no open database connection, click **OK** to proceed.

Chapter 7
Managing System Groups

In this chapter, you will learn about:

- Discover Modes
- Adding Computers
- Removing Computers
- Removing Unmanaged Systems
- Logical System Groups

Discover Modes

System Manager adds Domains and Computers in your enterprise in two modes. You can switch discover modes anytime you wish.

Auto Discover Mode

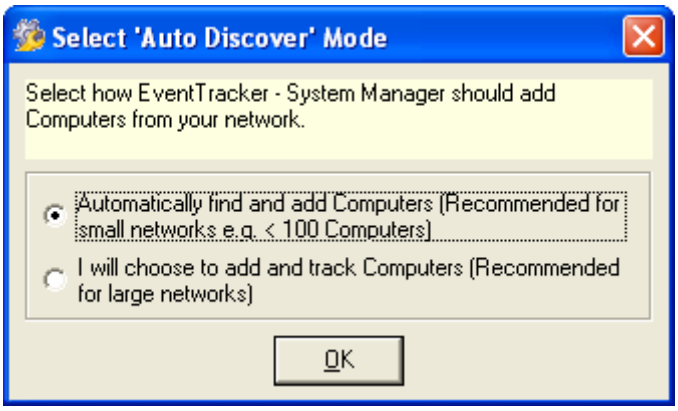
The Auto Discovery mode detects and adds all systems found on all trusted domains. The auto discovery process includes an initial quick detection for systems and a background search for more systems. On completion of the background discovery process it prompts the user to refresh the System Manager to get an updated list of systems. This mode is easy to use and is recommended for networks having less than 100 systems.

To set auto discover mode

1. Open the System Manager.
2. Click the **File** menu and select the **Select 'Auto Discover' Mode** option.

   System Manager displays the Select 'Auto Discover' Mode dialog box.

Figure 122 Select 'Auto Discover' Mode


Select 'Auto Discover' Mode
Select how EventTracker - System Manager should add Computers from your network.
Automatically find and add Computers (Recommended for small networks e.g. < 100 Computers)
I will choose to add and track Computers (Recommended for large networks)
OK

3. Click the **Automatically find and add Computers [Recommended for small networks e.g. < 100 Computers]** option.
4. Click **OK**.

   System Manager automatically starts adding Domains and computers.

Manual Mode

Unlike in Auto Discover Mode, System Manager will not discover any Domains or computers in this mode. You have to add them manually. Had you switched from

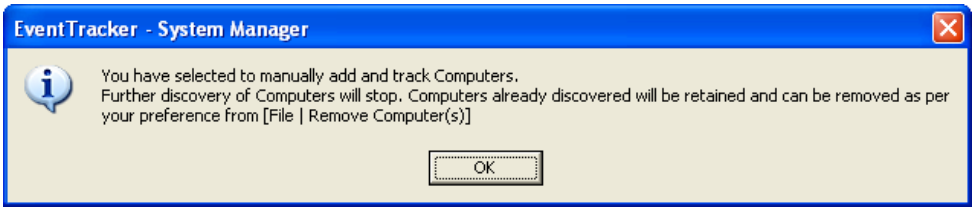
Auto to Manual mode, System Manager will retain previously discovered Domains and Computers.

To add computers manually

1. Select the **I will choose to add and track Computers (Recommended for large networks)** option in the Select 'Auto Discover' Mode window.
2. Click **OK**.

   System Manager displays the EventTracker – System Manager confirmation message box.

Figure 123 Set the option to add computers manually – message box


EventTracker - System Manager
You have selected to manually add and track Computers.
Further discovery of Computers will stop. Computers already discovered will be retained and can be removed as per your preference from [File | Remove Computer(s)]
OK

3. Click **OK**.

> **Note**
>
> In addition to the above, an option is also provided to either perform this search in the background or in the foreground. Performing the search in the background allows the user to proceed with other tasks on the System Manager.

Adding Computers

In Auto Discover Mode, the System Manager automatically discovers Domains and Computers when you keep adding them in your enterprise. All you need to do is to refresh the System Manager. But in Manual Mode, you have to add them explicitly. This section helps you add Computer(s) when the System Manager is in Manual Mode.

Adding a single Computer

This option enables you to add a computer.

To add a single computer

1. Open the System Manager.

2 Click the **File** menu and select the **Find/Add Computer(s)** option

(OR)

Click **Search Computers** on the toolbar.

(OR)

Press **F** holding **Ctrl** key on your keyboard.

System Manager displays the Add Computer(s) dialog box.

Figure 124 Add Computer(s) – Add a single computer

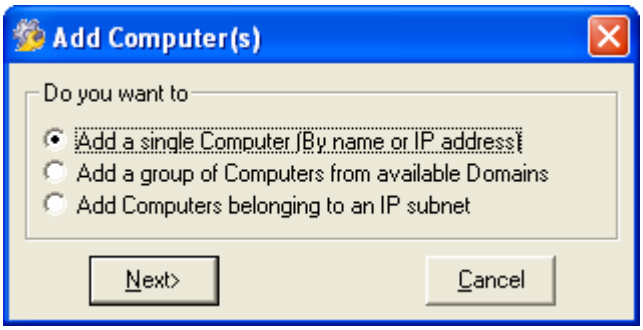

Add Computer(s)
Do you want to
Add a single Computer [By name or IP address]
Add a group of Computers from available Domains
Add Computers belonging to an IP subnet
Next>
Cancel

Table 30

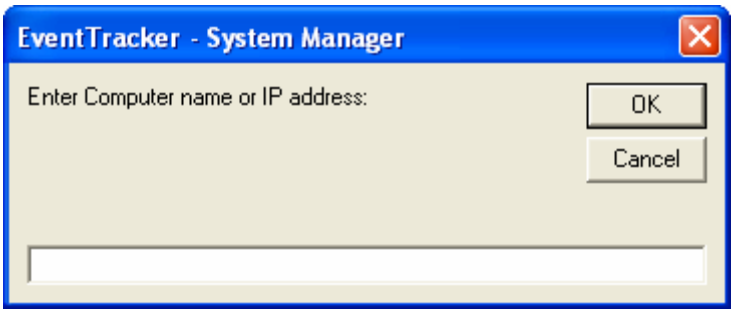
Field	Description
Add a single Computer [By name or IP address]	Select this option to add a single computer.
Add a group of Computers from available Domains	Select this option to add a group of computers.
Add Computers belonging to an IP subnet	Select this option to add computers from an IP subnet.

3 Click the **Add a single Computer [By name or IP address]** option.

4 Click **Next>**.

System Manager displays the EventTracker System Manager dialog box.

Figure 125 Add Computer (s) - Add a single computer

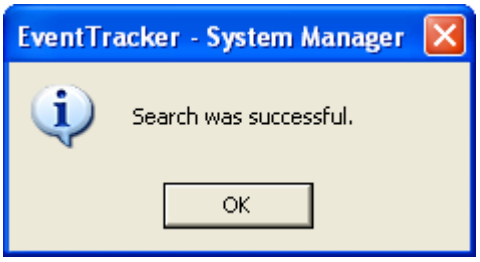


5 Type the computer name you want to add in the Group.

6 Click **OK**.

System Manager displays the EventTracker – System Manager message box.

Figure 126 Add Computers – message box



7 Click **OK**.

8 Edit the appropriate Domain and add the Computer to that Domain.

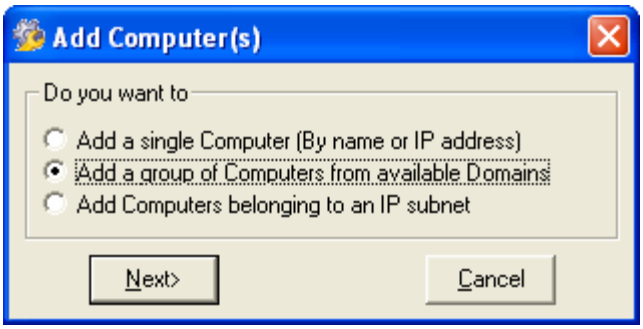
Adding a group of Computers

This option enables you to add a group of Computers. Note that it is possible to add Computers only with available Domains. As mentioned earlier, System Manager will be in Auto Discover Mode by default. Later on you switched the Discover Mode to Manual and added Computer(s) to a particular Domain, say Domain A. Since the System Manager is Manual Discover Mode, it cannot discover newly added Computer(s) by itself. In this scenario you can utilize this option to add those new Computer(s) to Domain A.

To add a group of computers

1 Select the **Add a group of Computers from available Domains** option in the **Add Computer(s)** window.

Figure 127 Add Computer(s) window – Add a group of computers


Add Computer(s)
Do you want to
Add a single Computer (By name or IP address)
Add a group of Computers from available Domains
Add Computers belonging to an IP subnet
Next>
Cancel

2 Click **Next>**.

System Manager displays the Select Criteria dialog box.

Figure 128 Select Criteria – Add a group of computers

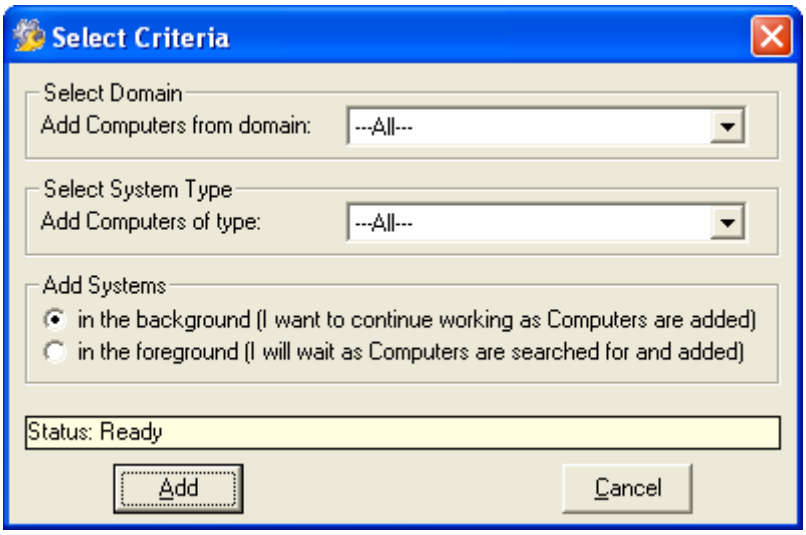


Table 31

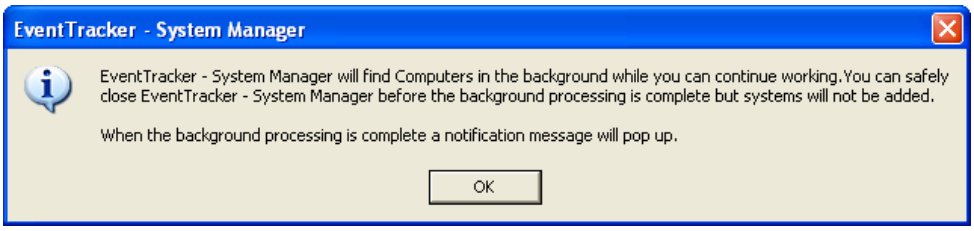
Field	Description
Select Domain	This drop-down list lists the available Domains. Select a Domain from where you want to add the computers, from this drop-down list. When you select --All-- option, System Manager will discover all the Computers and adds them up in their respective Domains.
Select System Type	Select a system type from the drop-down list. When you select --All—option, System Manager discovers all the Computers irrespective of their O/S type and adds them up in their respective Domains.
Add Systems	Search and add options can be done either in the background while you can continue with your work or in the foreground if you are interested to know about the search progress.

3 Select appropriate options.

4 Click **Add**.

If you select the **in the background (I want to continue working as Computers are added)** option, System Manager displays the EventTracker – System Manager message box.

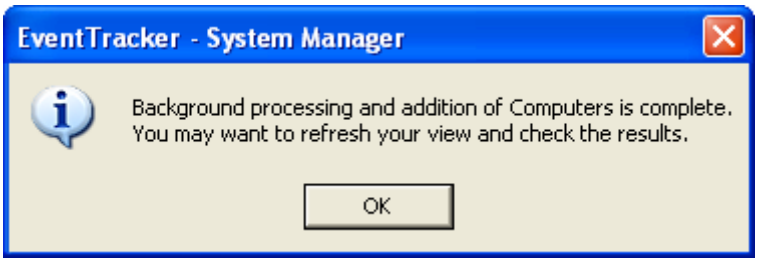
Figure 129 Add a group of computers – message box


EventTracker - System Manager
EventTracker - System Manager will find Computers in the background while you can continue working. You can safely close EventTracker - System Manager before the background processing is complete but systems will not be added.
When the background processing is complete a notification message will pop up.
OK

5 Click **OK**.

System Manager displays the EventTracker – System Manager message box after adding the computers.

Figure 130 Add a group of computers – message box


EventTracker - System Manager
Background processing and addition of Computers is complete.
You may want to refresh your view and check the results.
OK

6 Click **OK**.

7 Refresh the System Manager.

Note

If you select the in the foreground (I will wait as Computers are searched for and added) option, EventTracker displays the message in the status bar of the Select Criteria window as "The EventTracker System Manager is finding Computers". Computers in the selected group are added to the domain.

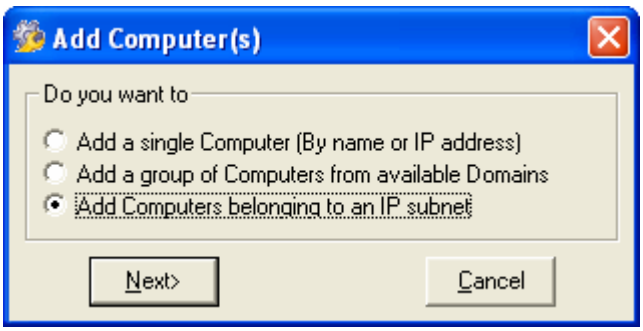
Adding a group of Computers from an IP subnet

This option enables you to add computers from an IP subnet.

To add computers from an IP subnet

1. Select the domain for which you want to add computes, in the left pane.
2. Click the **Add Computers belonging to an IP subnet** option in the **Add Computer(s)** window.

Figure 131 Add Computer(s) – Add computers from an IP subnet


Add Computer(s)
Do you want to
Add a single Computer (By name or IP address)
Add a group of Computers from available Domains
Add Computers belonging to an IP subnet
Next>
Cancel

3. Click **Next>**.

   System Manager displays the Add Subnet dialog box.

Figure 132 Add Subnet

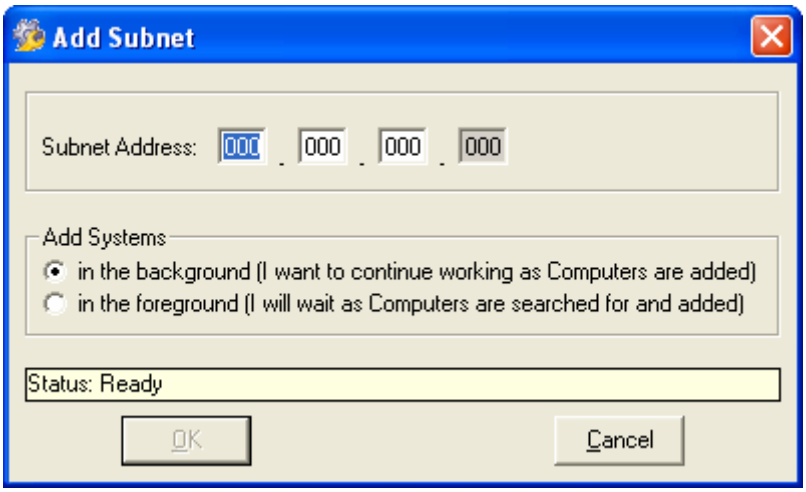

Add Subnet
Subnet Address: 000 . 000 . 000 . 000
Add Systems
in the background (I want to continue working as Computers are added)
in the foreground (I will wait as Computers are searched for and added)
Status: Ready
OK
Cancel

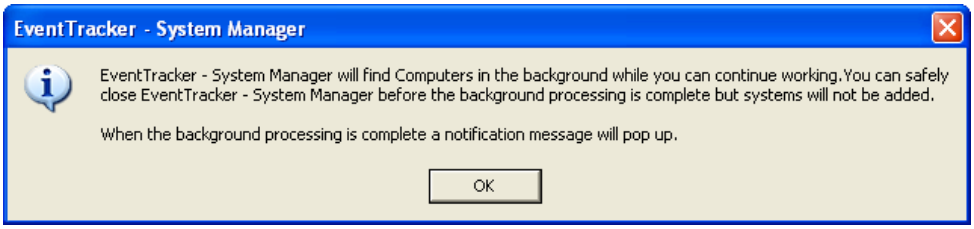
Table 32

Field	Description
Subnet Address	Type the IP address in these fields.
Add Systems	The options are in the background (I want to continue working as Computers are added) and in the foreground (I will wait as Computers are searched for and added).

4. Type appropriately in the relevant fields.
5. Click **OK**.

If you select the in the background (I want to continue working as Computers are added) option, System Manager displays the EventTracker – System Manager message box.

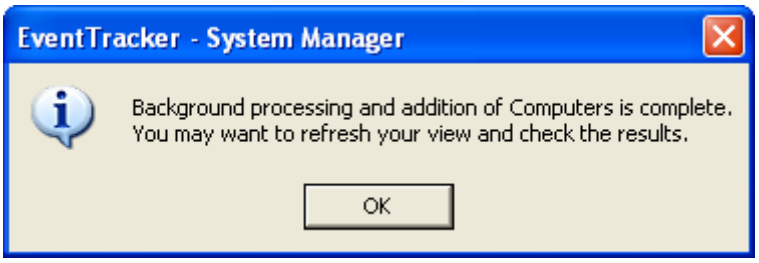
Figure 133 Add Computers– Add computers from an IP subnet


EventTracker - System Manager
EventTracker - System Manager will find Computers in the background while you can continue working.You can safely close EventTracker - System Manager before the background processing is complete but systems will not be added.
When the background processing is complete a notification message will pop up.
OK

6 Click **OK**.

System Manager displays the EventTracker - System Manager message box after adding the computers.

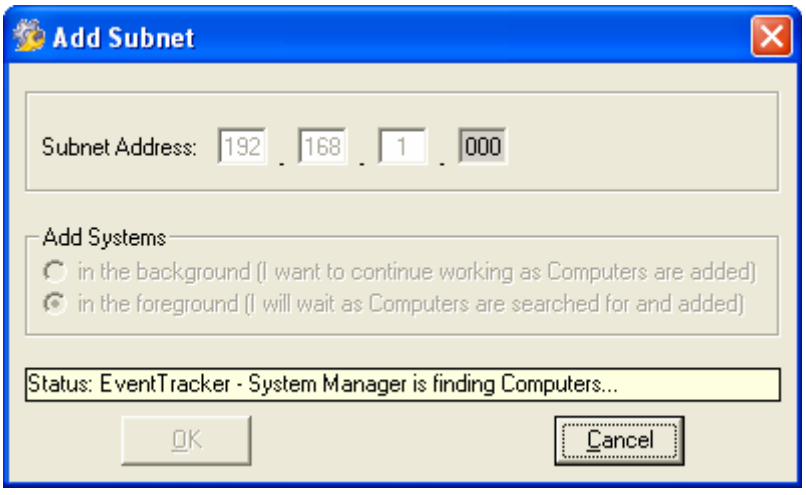
Figure 134 Add computers from an IP subnet – message box


EventTracker - System Manager
Background processing and addition of Computers is complete.
You may want to refresh your view and check the results.
OK

7 Click **OK**.

If you select the **in the foreground (I will wait as Computers are searched for and added)** option, System Manager displays the Add Subnet message box.

Figure 135 Add Subnet – Add systems in the foreground


Add Subnet
Subnet Address: 192 . 168 . 1 . 000
Add Systems
in the background (I want to continue working as Computers are added)
in the foreground (I will wait as Computers are searched for and added)
Status: EventTracker - System Manager is finding Computers...
OK
Cancel

8 Refresh the System Manager. The computers are added to the selected domain.

Removing Computers

You can either remove Computers when System Manager is in Auto or in Manual discover mode.

Removing Computers – Auto Discover Mode

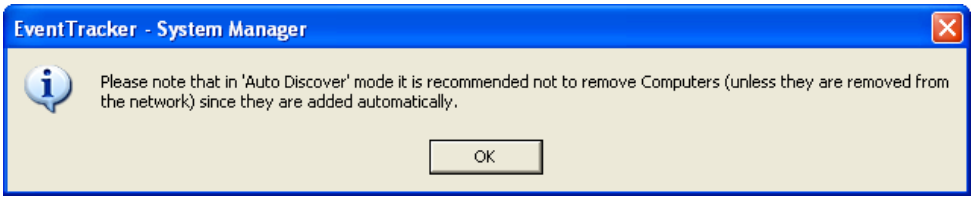
This option enables you to remove computers when the System Manager is in Auto Discover Mode.

To remove computers

1. Open the System Manager.
2. Click the **File** menu and select the **Remove Computer(s)** option.

   System Manager displays the EventTracker – System Manager message box.

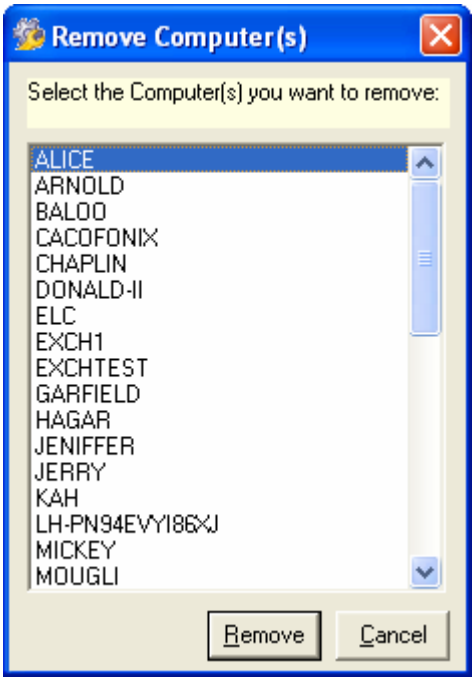
Figure 136 Remove Computers – message box


EventTracker - System Manager
Please note that in 'Auto Discover' mode it is recommended not to remove Computers (unless they are removed from the network) since they are added automatically.
OK

3. Click **OK** to continue removing the computers.

   System Manager displays the Remove Computer(s) dialog box.
4. Select the computer(s) that you want to remove.

Figure 137 Remove Computer(s)

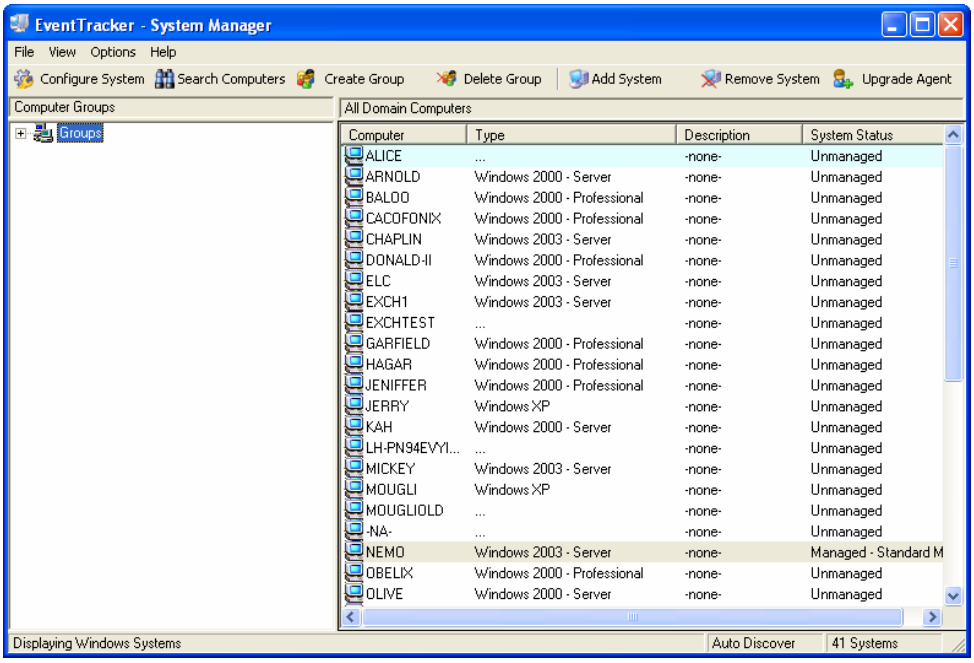


5 Click **Remove**.

System Manager removes the selected Computer.

6 Refresh the System Manager. System Manager discovers the removed computer(s).

Figure 138 System Manager


EventTracker - System Manager
File View Options Help
Configure System
Search Computers
Create Group
Delete Group
Add System
Remove System
Upgrade Agent
Computer Groups
Groups
All Domain Computers
Computer
Type
Description
System Status
ALICE ... -none- Unmanaged
ARNOLD Windows 2000 - Server -none- Unmanaged
BALOO Windows 2000 - Professional -none- Unmanaged
CACOFONIX Windows 2000 - Professional -none- Unmanaged
CHAPLIN Windows 2003 - Server -none- Unmanaged
DONALD-II Windows 2000 - Professional -none- Unmanaged
ELC Windows 2003 - Server -none- Unmanaged
EXCH1 Windows 2003 - Server -none- Unmanaged
EXCHTEST ... -none- Unmanaged
GARFIELD Windows 2000 - Professional -none- Unmanaged
HAGAR Windows 2000 - Professional -none- Unmanaged
JENIFFER Windows 2000 - Professional -none- Unmanaged
JERRY Windows XP -none- Unmanaged
KAH Windows 2000 - Server -none- Unmanaged
LH-PN94EVYI... ... -none- Unmanaged
MICKEY Windows 2003 - Server -none- Unmanaged
MOUGLI Windows XP -none- Unmanaged
MOUGLIOLD ... -none- Unmanaged
-NA- ... -none- Unmanaged
NEMO Windows 2003 - Server -none- Managed - Standard M
OBELIX Windows 2000 - Professional -none- Unmanaged
OLIVE Windows 2000 - Server -none- Unmanaged
Displaying Windows Systems
Auto Discover
41 Systems

Removing Computers - Manual Mode

This option enables you to remove computers when the System Manager is in Manual Discover Mode.

To remove Computer(s)

1. Open the System Manager.
2. Click the **File** menu and select the **Remove Computer(s)** option.

   System Manager displays the Remove Computer(s) dialog box.

> **Note**
>
> System Manager automatically discovered the Computers listed in the Remove Computer(s) dialog box. Remove button is disabled by default. System Manager enables it only when you select Computer(s) from the list.

3. Select the Computer(s) that you want to remove.
4. Click **Remove**.

   System Manager removes the selected computer(s).

5 Refresh the System Manager.

Note

Since the System Manager is in Manual mode, it could not discover the removed Computer. It is obvious that you have to add the removed Computer(s) manually.

Removing Unmanaged Systems

This option helps you remove unmanaged systems from the view as well as from the database. The discovery of systems in your enterprise should be in "Manual" mode and not in "Auto Discover" mode. In Auto discover mode if you remove the system, it will be removed only for that instance and when you refresh the System Manager, the removed systems will be discovered and get populated to the list.

Example scenario: Suppose you were monitoring a system and that system exists in two Groups namely TOONS and MY GROUP. Now you want to remove that unmanaged system from the All Domain Computers list in the right pane, do the following.

To remove unmanaged systems

1 Click the **File** menu and select the **Select 'Auto Discover' Mode** option.

System Manager displays the Select 'Auto Discover' Mode dialog box.

2 Select the **I will choose to add and track Computers (Recommended for large networks)** option and then click **OK**.

System Manager displays the EventTracker – System Manager message box.

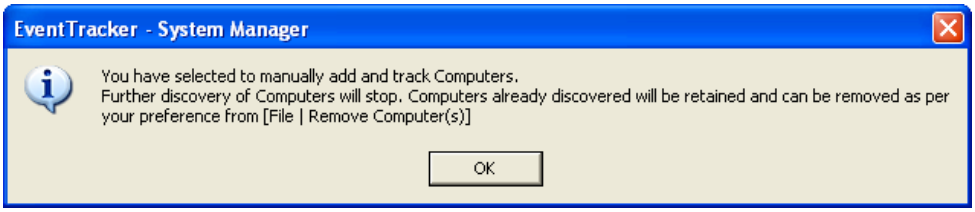
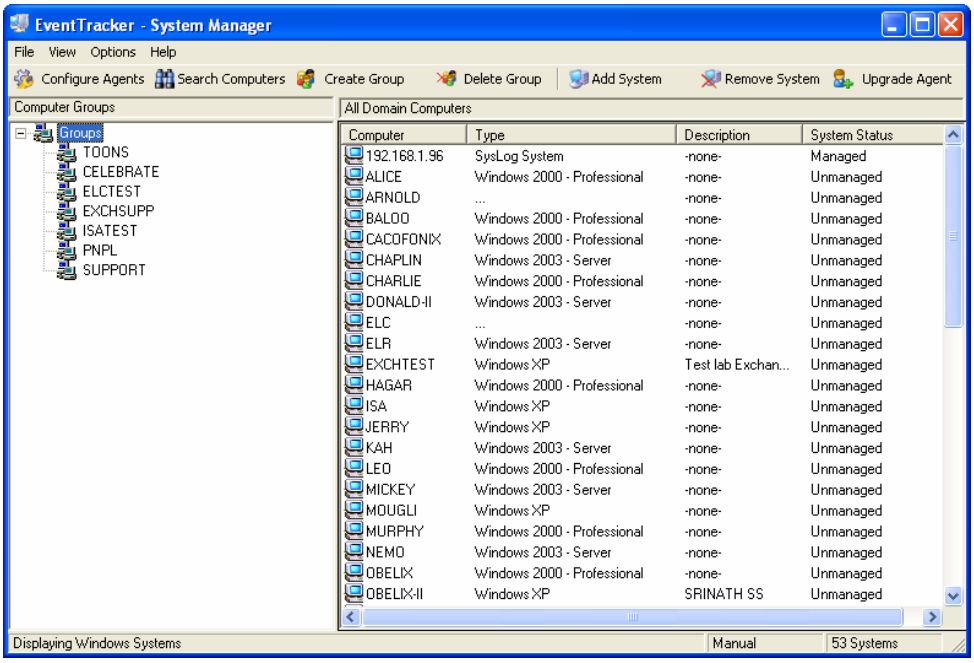

EventTracker - System Manager
You have selected to manually add and track Computers.
Further discovery of Computers will stop. Computers already discovered will be retained and can be removed as per your preference from [File | Remove Computer(s)]
OK

Figure 139
EventTracker - System Manager message box

3 Click **OK**.

4 Expand the Groups tree in the left pane.

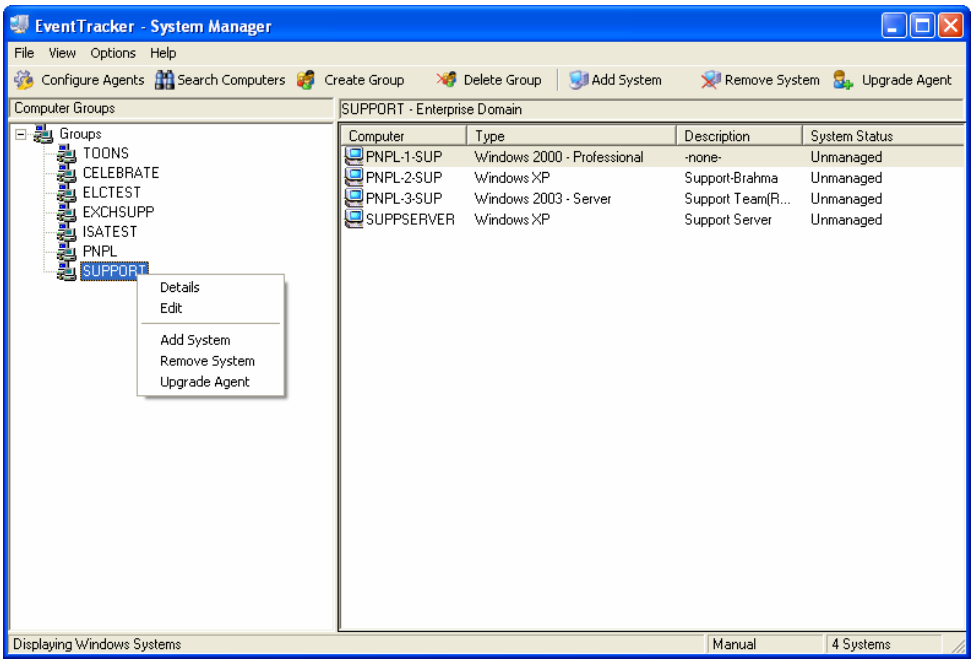
Figure 140 EventTracker - System Manager left pane


EventTracker - System Manager
File View Options Help
Configure Agents Search Computers Create Group Delete Group Add System Remove System Upgrade Agent
Computer Groups
All Domain Computers
Groups
TOONS
CELEBRATE
ELCTEST
EXCHSUPP
ISATEST
PNPL
SUPPORT
Computer Type Description System Status
192.168.1.96 SysLog System -none- Managed
ALICE Windows 2000 - Professional -none- Unmanaged
ARNOLD ... -none- Unmanaged
BALOO Windows 2000 - Professional -none- Unmanaged
CACOFONIX Windows 2000 - Professional -none- Unmanaged
CHAPLIN Windows 2003 - Server -none- Unmanaged
CHARLIE Windows 2000 - Professional -none- Unmanaged
DONALD-II Windows 2003 - Server -none- Unmanaged
ELC ... -none- Unmanaged
ELR Windows 2003 - Server -none- Unmanaged
EXCHTEST Windows XP Test lab Exchan... Unmanaged
HAGAR Windows 2000 - Professional -none- Unmanaged
ISA Windows XP -none- Unmanaged
JERRY Windows XP -none- Unmanaged
KAH Windows 2003 - Server -none- Unmanaged
LEO Windows 2000 - Professional -none- Unmanaged
MICKEY Windows 2003 - Server -none- Unmanaged
MOUGLI Windows XP -none- Unmanaged
MURPHY Windows 2000 - Professional -none- Unmanaged
NEMO Windows 2003 - Server -none- Unmanaged
OBELIX Windows 2000 - Professional -none- Unmanaged
OBELIX-II Windows XP SRINATH SS Unmanaged
Displaying Windows Systems
Manual
53 Systems

5 Right-click **Support**.

System Manager displays the shortcut menu.

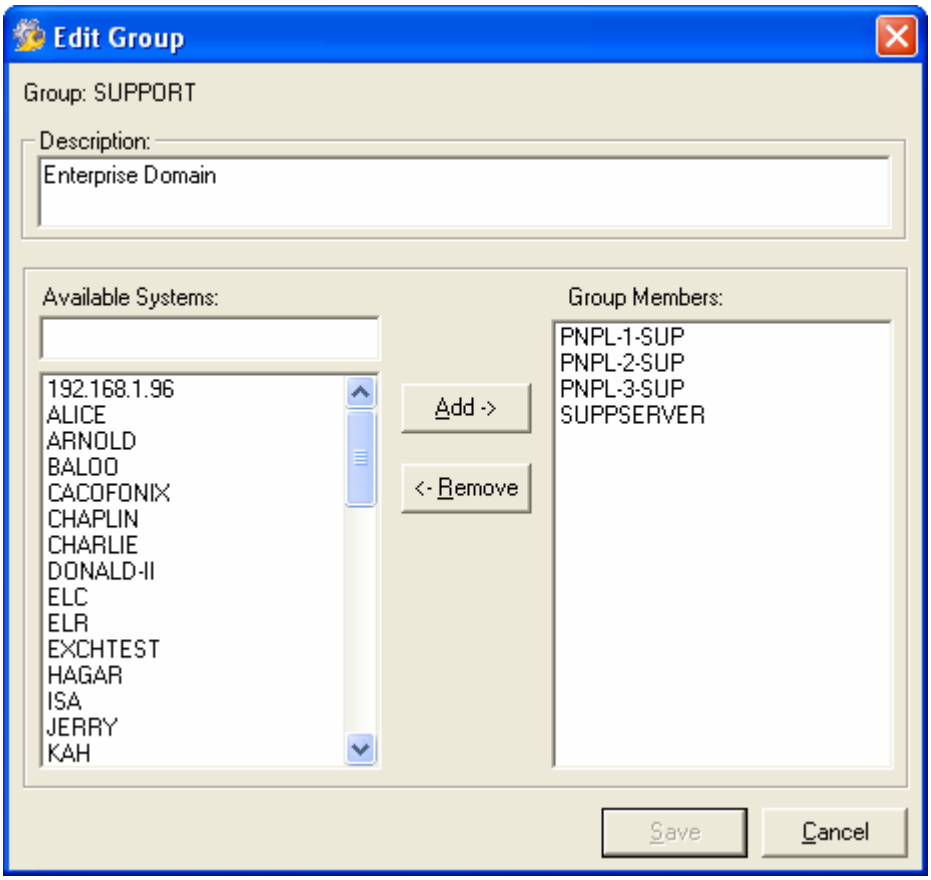
Figure 141 EventTracker - System Manager left pane



From the shortcut menu, choose **Edit**.

System Manager displays the Edit Group window.

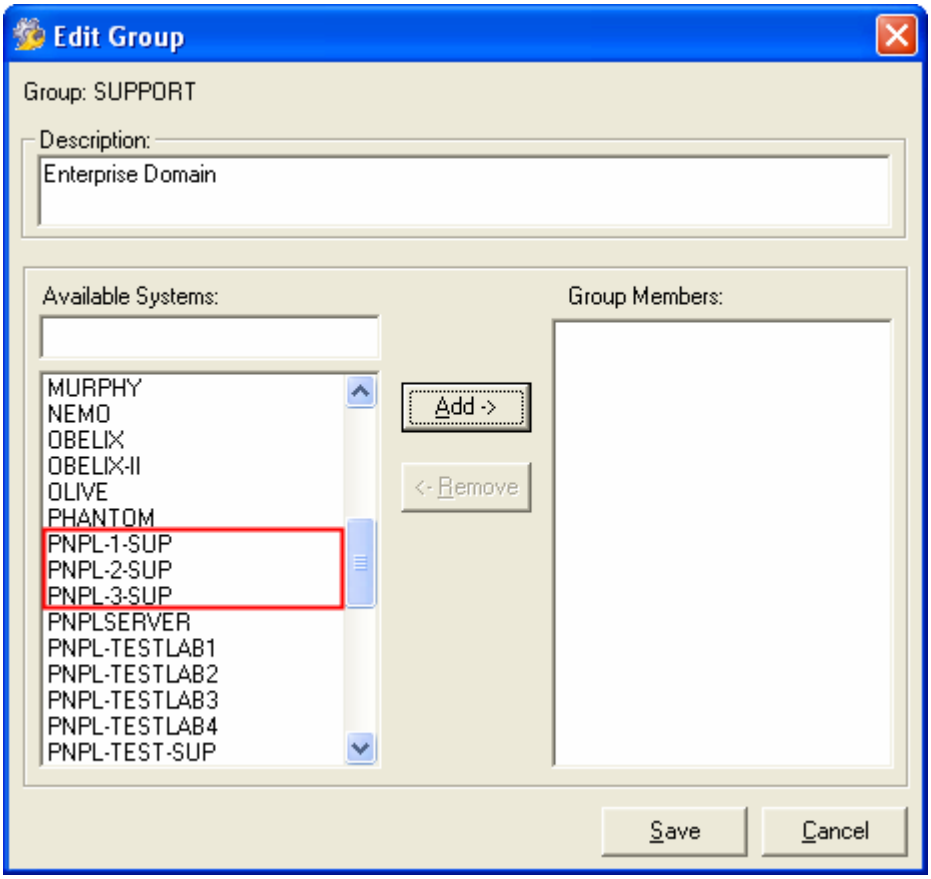
Figure 142 Edit Group window



6 Select the system from the **Group Members** list and then click **<Remove**.

System Manager displays the Edit Group window.

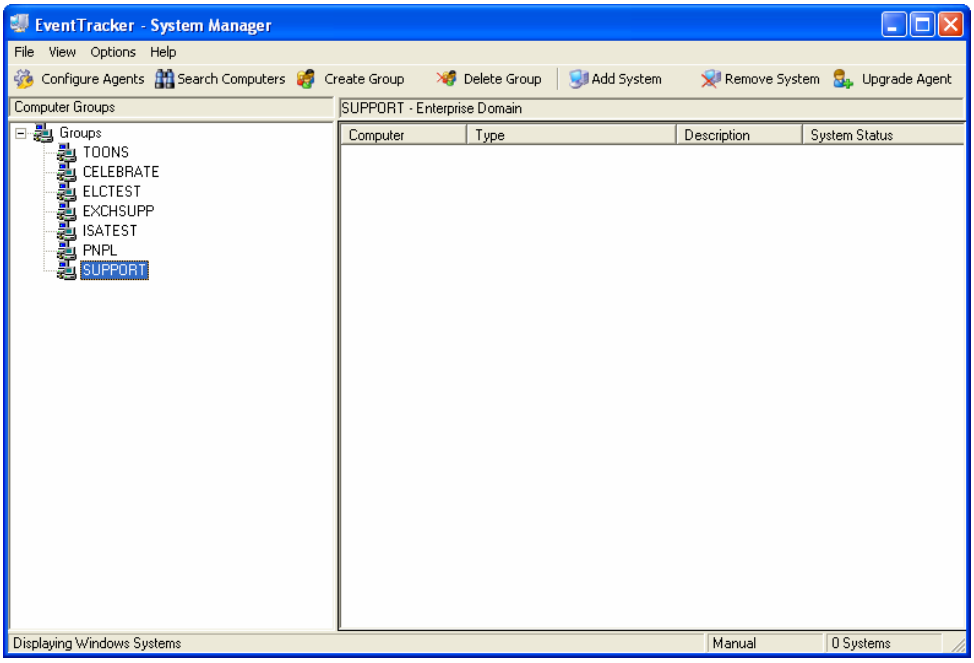
Figure 143 Edit Group



7 Click **Save**.

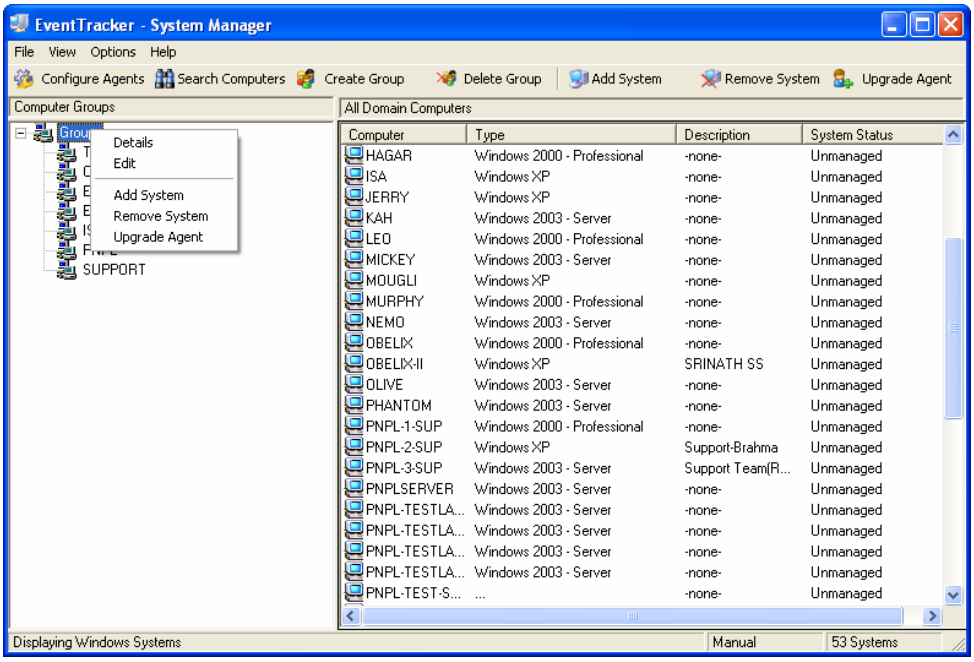
System Manager removes the selected system and displays the System Manager.

Figure 144
EventTracker System Manager



8 To remove the system from all the groups, right-click Groups in the left pane.

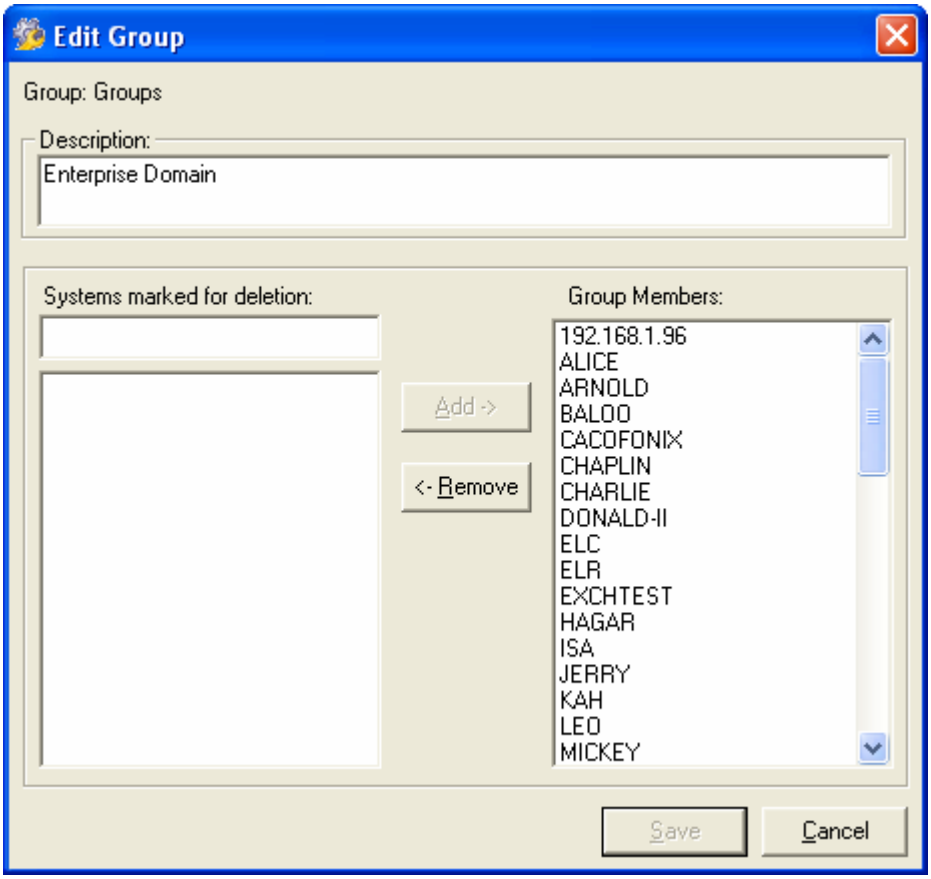
Figure 145
EventTracker - System Manager left pane


EventTracker - System Manager
File View Options Help
Configure Agents
Search Computers
Create Group
Delete Group
Add System
Remove System
Upgrade Agent
Computer Groups
All Domain Computers
Details
Edit
Add System
Remove System
Upgrade Agent
SUPPORT
Computer
Type
Description
System Status
HAGAR Windows 2000 - Professional -none- Unmanaged
ISA Windows XP -none- Unmanaged
JERRY Windows XP -none- Unmanaged
KAH Windows 2003 - Server -none- Unmanaged
LEO Windows 2000 - Professional -none- Unmanaged
MICKEY Windows 2003 - Server -none- Unmanaged
MOUGLI Windows XP -none- Unmanaged
MURPHY Windows 2000 - Professional -none- Unmanaged
NEMO Windows 2003 - Server -none- Unmanaged
OBELIX Windows 2000 - Professional -none- Unmanaged
OBELIX-II Windows XP SRINATH SS Unmanaged
OLIVE Windows 2003 - Server -none- Unmanaged
PHANTOM Windows 2003 - Server -none- Unmanaged
PNPL-1-SUP Windows 2000 - Professional -none- Unmanaged
PNPL-2-SUP Windows XP Support-Brahma Unmanaged
PNPL-3-SUP Windows 2003 - Server Support Team(R... Unmanaged
PNPLSERVER Windows 2003 - Server -none- Unmanaged
PNPL-TESTLA... Windows 2003 - Server -none- Unmanaged
PNPL-TESTLA... Windows 2003 - Server -none- Unmanaged
PNPL-TESTLA... Windows 2003 - Server -none- Unmanaged
PNPL-TESTLA... Windows 2003 - Server -none- Unmanaged
PNPL-TEST-S... ... -none- Unmanaged
Displaying Windows Systems
Manual
53 Systems

9 Click **Edit**.

System Manager displays the Edit Group window.

Figure 146 Edit Group



10 Select the systems from Group Members and then click **<-Remove**.

11 Click **Save**.

System Manager removes the selected systems from all the Groups if those systems exist in more than one Group.

Logical System Groups

Logical System Groups help you to monitor the Computers you are interested in. You can choose Computers based on the O/S type, IP subnet or pick them manually.

Creating a New Logical Group - System Type

This option enables you to create a new logical Group of systems based on system type.

To create a new logical group and add systems based on System Type

1. Open the Management console.
2. Click the **Configure** menu, and select the **Manage Systems** option

   (OR)

   Click **Manage Systems** on the toolbar.

   System Manager displays the System Manager.
3. Click the **File** menu, and select the **Create Group** option

   (OR)

   Click **Create Group** on the toolbar.

   System Manager displays the Create Group dialog box.

Figure 147 Create Group – System Type

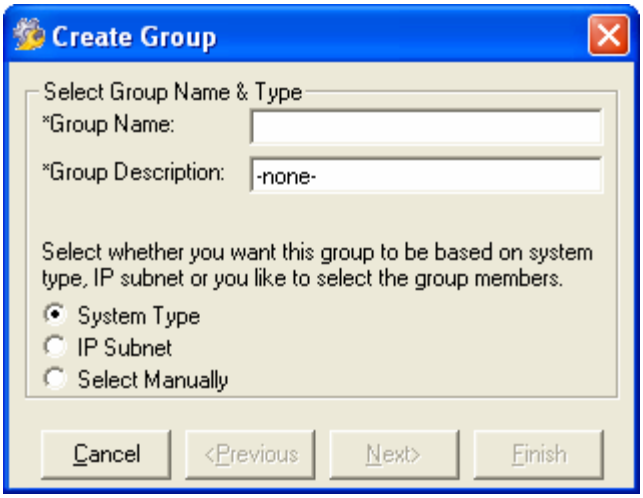
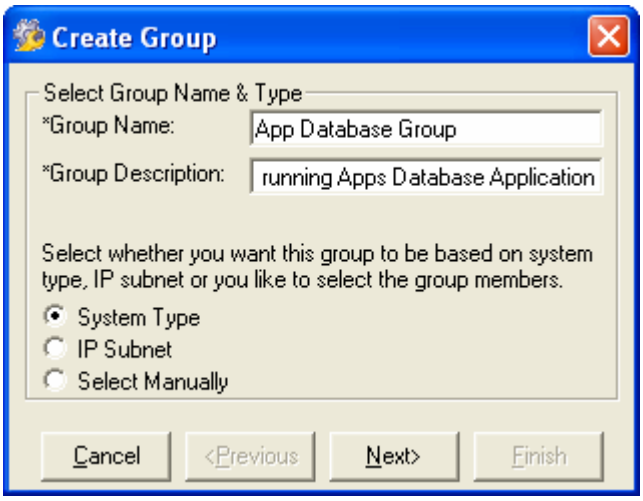


Table 33

Field (Field * marked are mandatory)	Description
*** Group Name**	Type the group name in this field. The group name should be unique.
*** Group Description**	Type the group description in this field.
Group Type	Select the group type option. The options are System Type, IP Subnet and Select Manually. **System Type** – Enables you to add the selected system type to the group. **IP Subnet** – Enables you to add the IP subnet to the group. **Select Manually** – Enables you to add the systems manually from the available list to the group.

4 Type appropriately in the relevant fields.

Figure 148 Create Group – System Type


Create Group
Select Group Name & Type
*Group Name:
App Database Group
*Group Description:
running Apps Database Application
Select whether you want this group to be based on system type, IP subnet or you like to select the group members.
System Type
IP Subnet
Select Manually
Cancel
<Previous
Next>
Finish

5 Click **Next>**.

If you select the **System Type** option, System Manager displays the Create Group dialog box.

Figure 149 Create Group – System Type

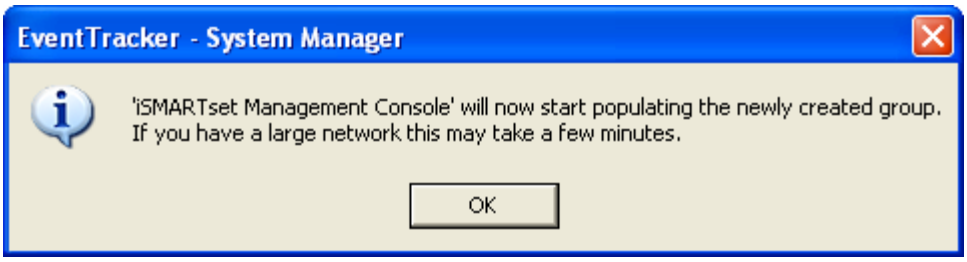
Create Group
Select System Type
Select the system type from the list of supported types. All systems of the following type will become members of this group.
Servers - 2003/2000/NT
Cancel
<Previous
Next>
Finish

6 Select the system type from the **Select System Type** drop-down list.

7 Click **Finish**.

System Manager displays the EventTracker – System Manager message box.

Figure 150 Create Group - message box


EventTracker - System Manager
'iSMARTset Management Console' will now start populating the newly created group.
If you have a large network this may take a few minutes.
OK

8 Click **OK**.

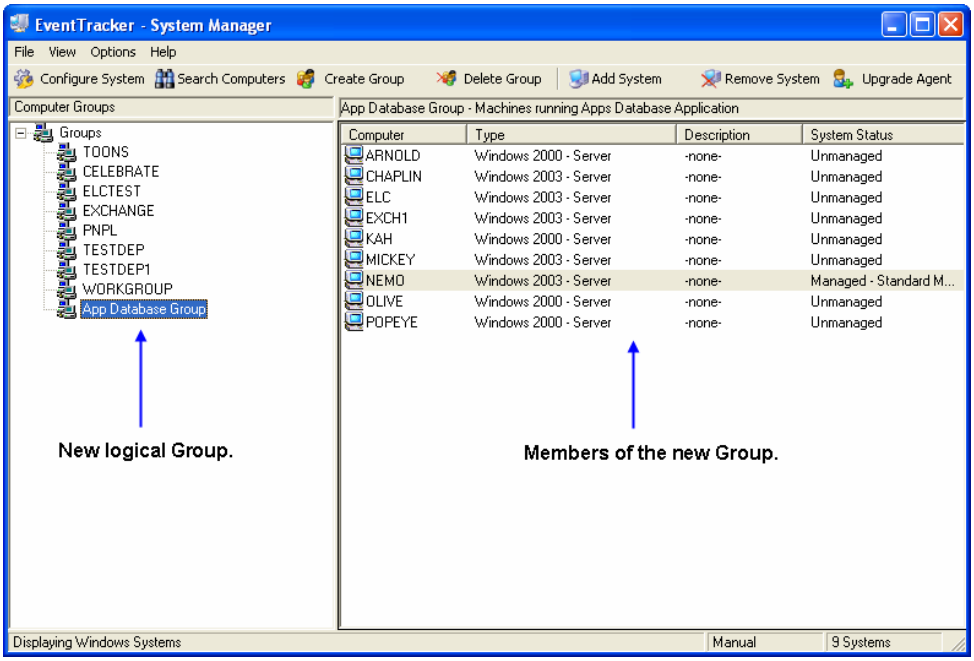
System Manager displays the EventTracker – System Manager message box after creating a group.

Figure 151 Create Group - message box

9 Click **OK**.

System Manager displays the EventTracker - System Manager with the newly created Group.

Figure 152 System Manager console after creating a group


EventTracker - System Manager
File View Options Help
Configure System Search Computers Create Group Delete Group Add System Remove System Upgrade Agent
Computer Groups
Groups
TOONS
CELEBRATE
ELCTEST
EXCHANGE
PNPL
TESTDEP
TESTDEP1
WORKGROUP
App Database Group
App Database Group - Machines running Apps Database Application
Computer Type Description System Status
ARNOLD Windows 2000 - Server -none- Unmanaged
CHAPLIN Windows 2003 - Server -none- Unmanaged
ELC Windows 2003 - Server -none- Unmanaged
EXCH1 Windows 2003 - Server -none- Unmanaged
KAH Windows 2000 - Server -none- Unmanaged
MICKEY Windows 2003 - Server -none- Unmanaged
NEMO Windows 2003 - Server -none- Managed - Standard M...
OLIVE Windows 2000 - Server -none- Unmanaged
POPEYE Windows 2000 - Server -none- Unmanaged
New logical Group.
Members of the new Group.
Displaying Windows Systems
Manual
9 Systems

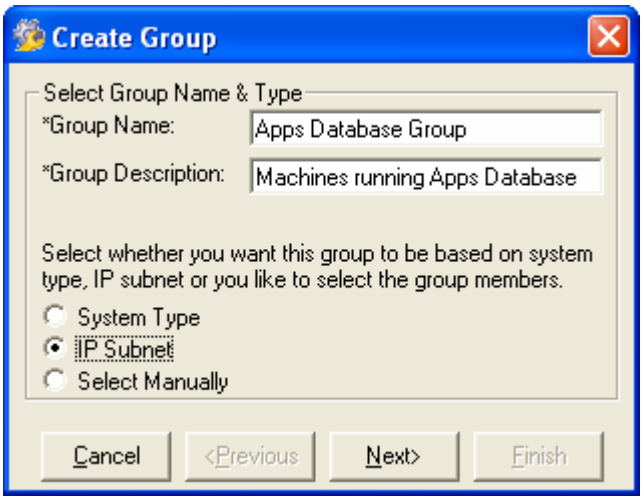
Creating a New Logical Group – IP Subnet

This option enables you to create a new logical Group of systems based on IP subnet.

To create a new logical group and add systems based on IP subnet

1 Select the **IP Subnet** option in the Create Group dialog box.

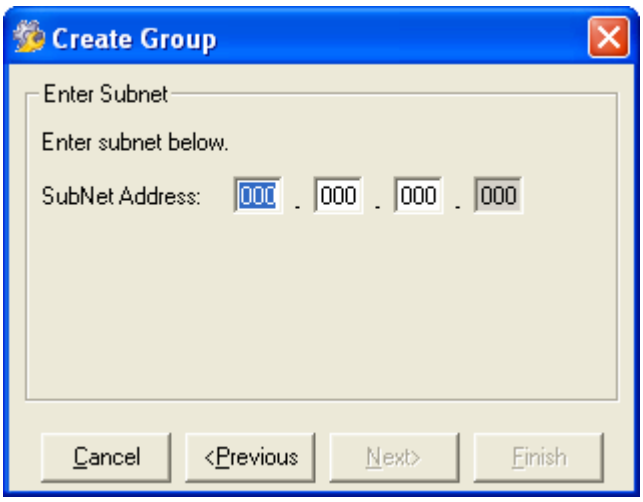
Figure 153 Create Group – IP Subnet


Create Group
Select Group Name & Type
*Group Name:
Apps Database Group
*Group Description:
Machines running Apps Database
Select whether you want this group to be based on system type, IP subnet or you like to select the group members.
System Type
IP Subnet
Select Manually
Cancel
<Previous
Next>
Finish

2 Click **Next>**.

System Manager displays the Create Group dialog box.

Figure 154 Create Group – IP Subnet

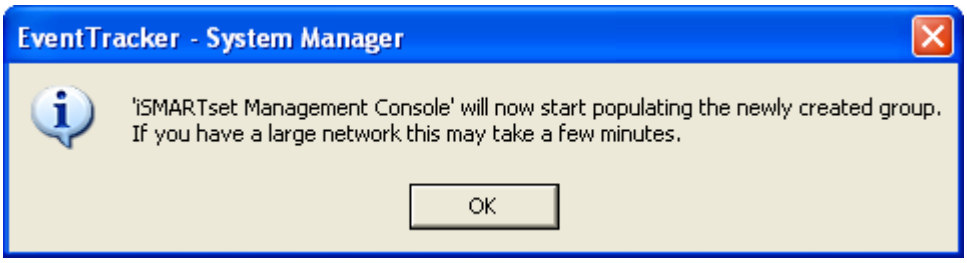


3 Type the **SubNet Address**.

4 Click **Finish**.

System Manager displays the EventTracker – System Manager message box.

Figure 155 Create Group – message box


EventTracker - System Manager
'iSMARTset Management Console' will now start populating the newly created group.
If you have a large network this may take a few minutes.
OK

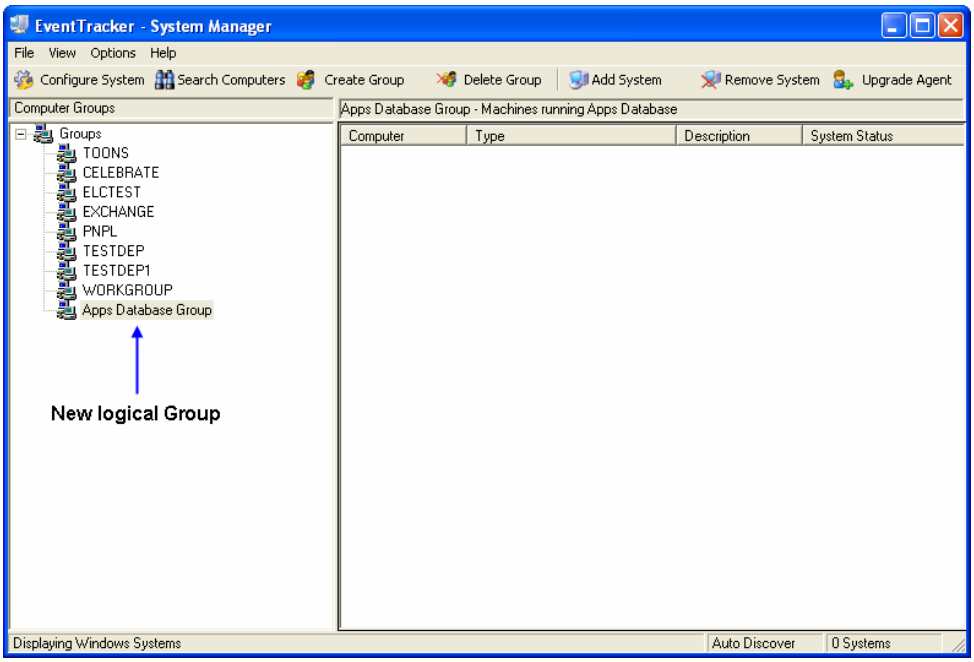
5 Click **OK**.

System Manager displays the EventTracker – System Manager message box after creating a group.

Figure 156 Create Group – message box

The created group is displayed in the left pane of the System Manager.

Figure 157 EventTracker – System Manager with newly created Group.



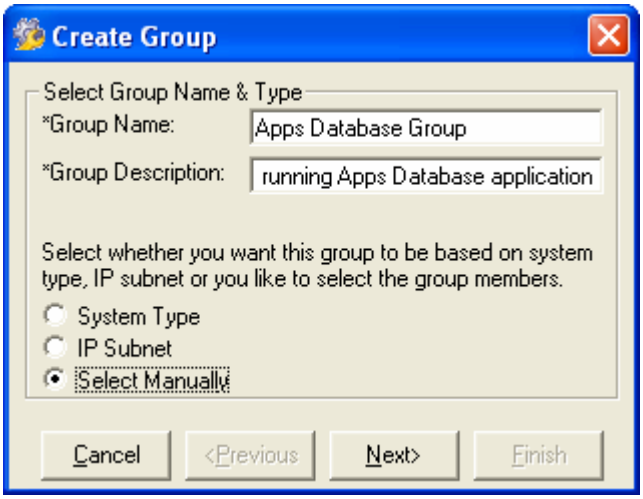
Creating a New Logical Group – Manual Selection

This option enables you to create a new logical Group of systems and manually add Computers to that Group.

To create a new logical group and add systems manually to that group

1 Select the **Select Manually** option in the Create Group window.

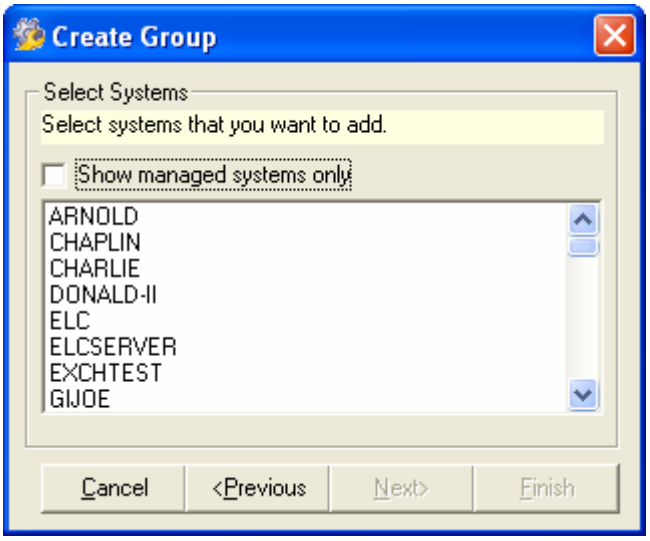
Figure 158 Create Group – Select Systems Manually


Create Group
Select Group Name & Type
*Group Name:
Apps Database Group
*Group Description:
running Apps Database application
Select whether you want this group to be based on system type, IP subnet or you like to select the group members.
System Type
IP Subnet
Select Manually
Cancel
<Previous
Next>
Finish

2 Click **Next>**.

System Manager displays the Create Group dialog box.

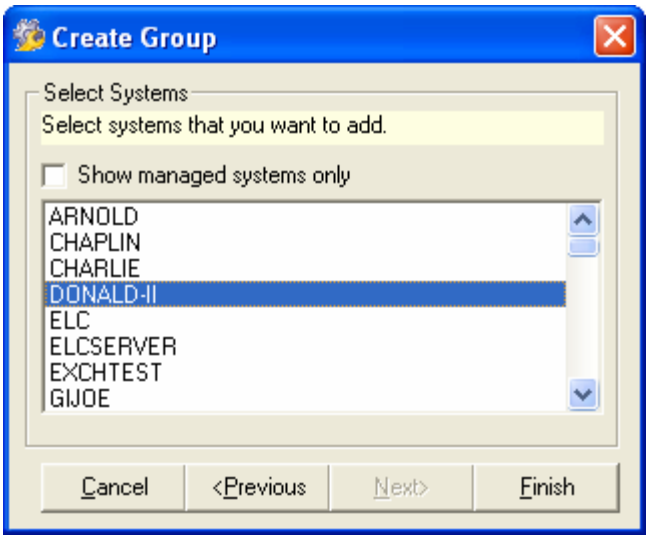
Figure 159 Create Group – Select Systems Manually



3 Select the **Show managed systems only** check box to view the systems managed by this manager.

4 Select the systems you want to add to the group from the list.

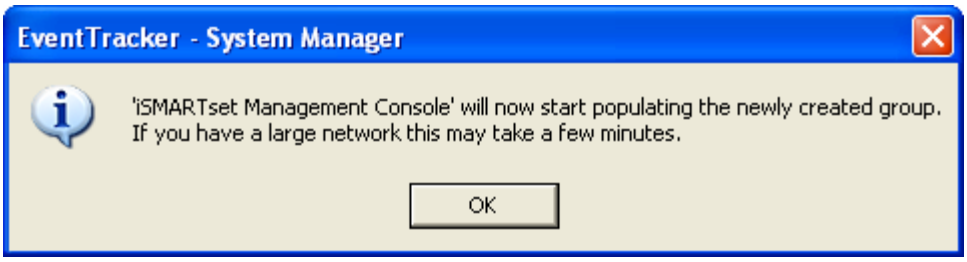
Figure 160 Create Group – Select Systems Manually



5 Click **Finish**.

System Manager displays the EventTracker – System Manager message box.

Figure 161 Create Group – message box


EventTracker - System Manager
'iSMARTset Management Console' will now start populating the newly created group.
If you have a large network this may take a few minutes.
OK

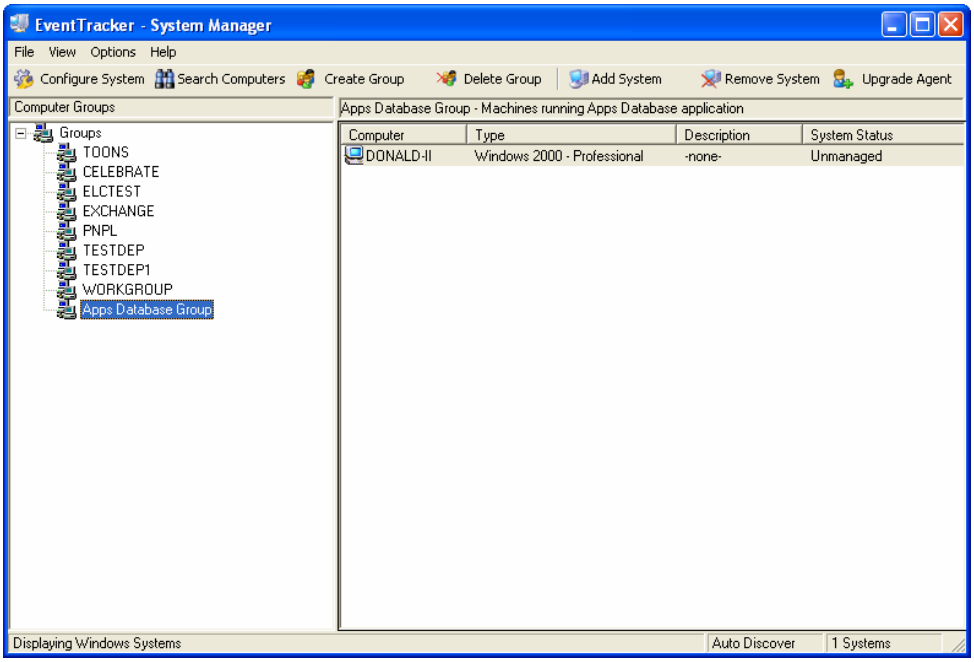
6 Click **OK**.

System Manager displays the EventTracker – System Manager message box after creating a group.

Figure 162 Create Group – message box

The created group is displayed in the left pane of the System Manager.

Figure 163 EventTracker – System Manager with newly created Group.



If the **Group Name** already exists, System Manager displays the EventTracker – System Manager message box.

Figure 164 Create Group – message box

7 Type a unique Group name and then click **OK** to continue creating the Group.

Modifying a Group

This option enables you to modify a Group.

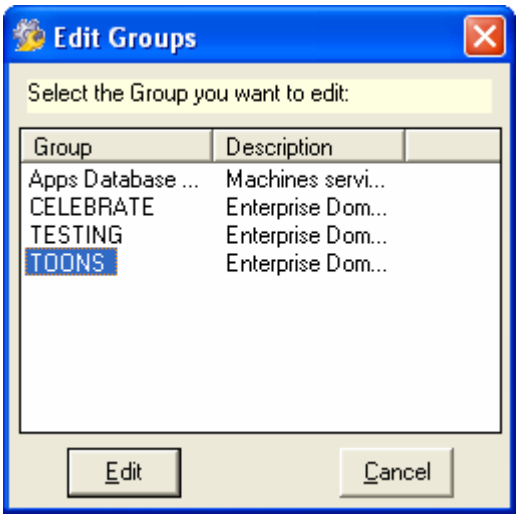
To modify a Group

1 Open the System Manager.

2 Click the **File** menu and select the **Edit Group** option.

System Manager displays the Edit Groups dialog box.

Figure 165 Edit Groups



3 Select the Group that you want to modify in the displayed list.

4 Click **Edit**.

System Manager displays the Edit Group dialog box.

Figure 166 Edit Group

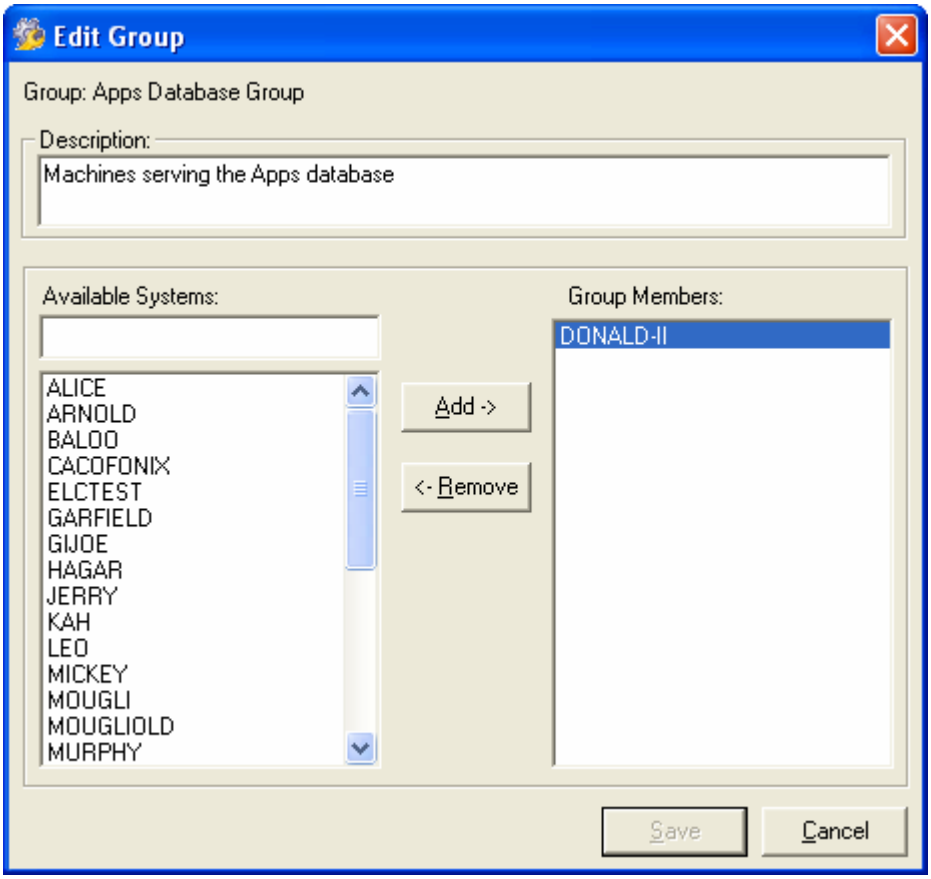


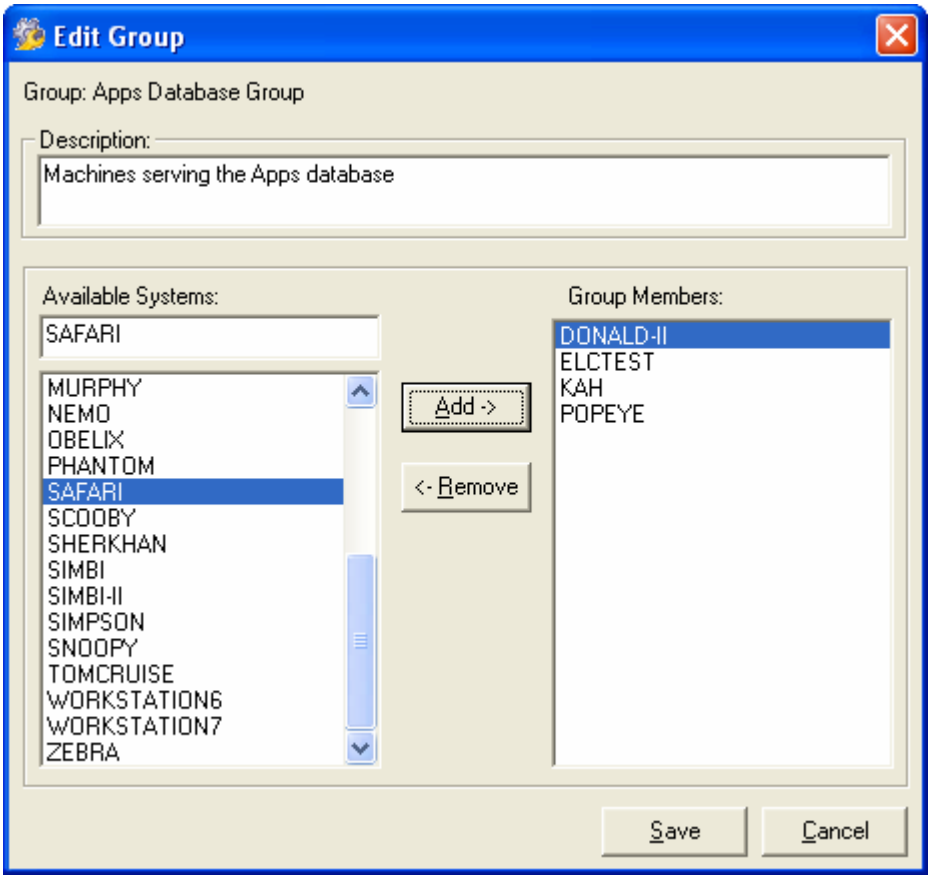
Table 34

Field	Description
Description	Type the system-related information in this field.
Group Members	Select the computer that you want to remove from the group. Click **<-Remove**.
Available Systems	Select the computer that you want to add to the group. Click **Add->**. The selected computer is added to the list of Group Members.

5 Type appropriately in the relevant fields.

System Manager displays the Edit Group dialog box.

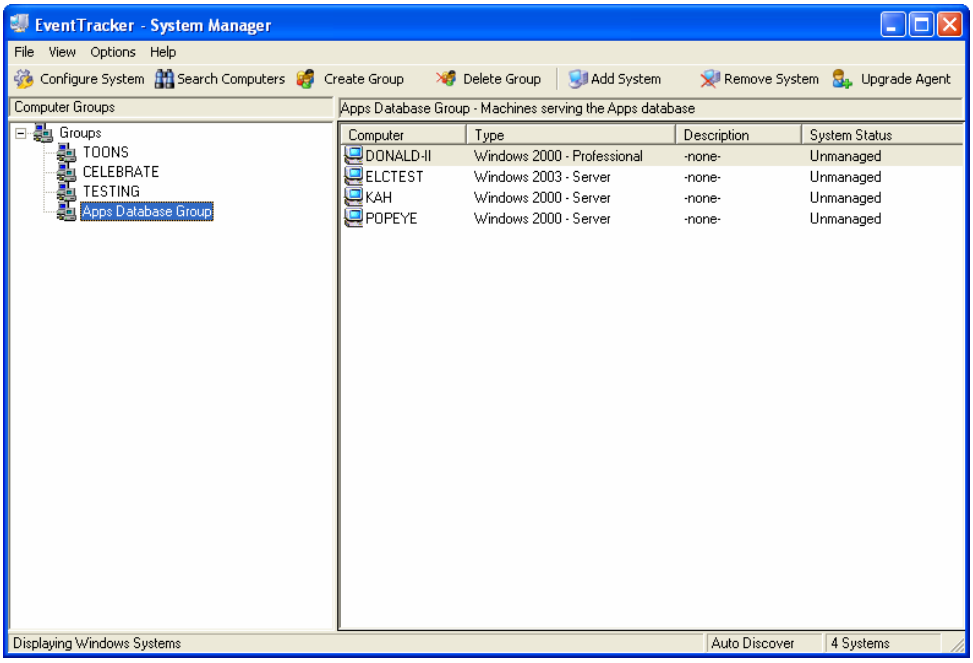
Figure 167 Edit Group



6 Click **Save**.

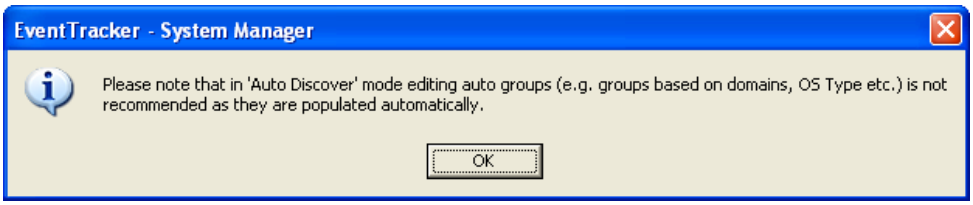
The modified group is displayed in the left pane of the System Manager.

Figure 168 EventTracker – System Manager with newly created Group.



Had you already selected the **Automatically find and add Computers (Recommended for small networks e.g.<100 Computers)** option in the **Auto Discover Mode** option, System Manager displays the EventTracker – System Manager message box.

Figure 169 Edit Group – message box


EventTracker - System Manager
Please note that in 'Auto Discover' mode editing auto groups (e.g. groups based on domains, OS Type etc.) is not recommended as they are populated automatically.
OK

7 Click **OK** to continue modifying the group.

Deleting a Group

This option enables you to delete an existing Group.

To delete a Group

1 Open the System Manager.

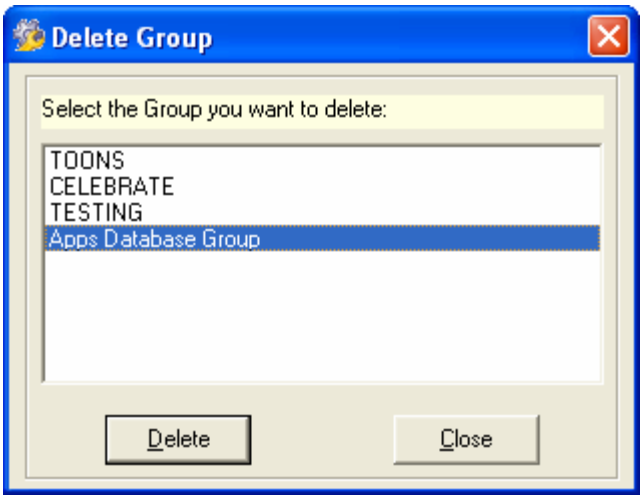
2 Click the **File** menu and select the **Delete Group** option

(OR)

Click **Delete Group** on the toolbar.

System Manager displays the Delete Group window.

Figure 170 Delete Group

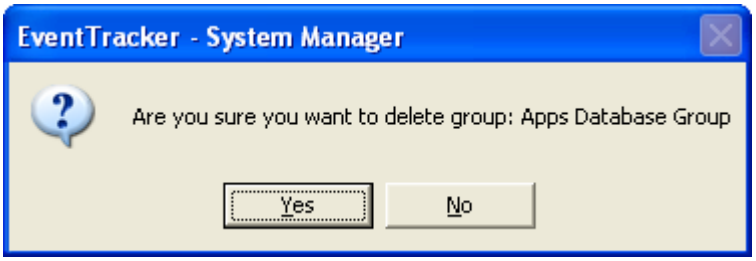


3 Select the Group that you want to delete in the displayed list.

4 Click **Delete**.

System Manager displays the EventTracker – System Manager confirmation message box.

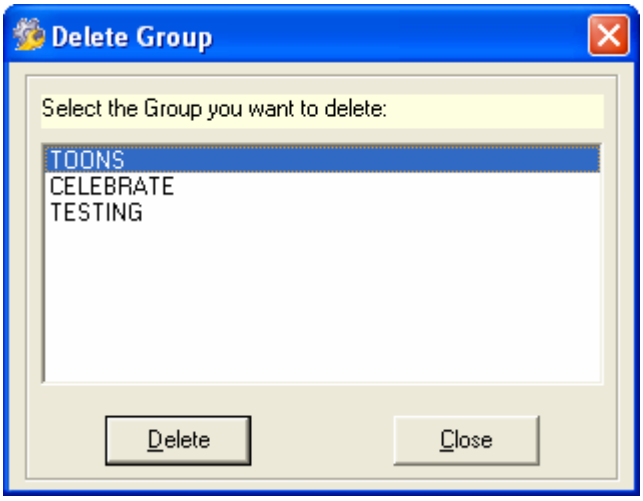
Figure 171 Delete Group – Confirmatory message box



5 Click **Yes**.

The selected Group is deleted from the list.

Figure 172 Delete Group



6 Click **Close**.

Had you selected the **Automatically find and add Computers (Recommended for small networks e.g.<100 Computers)** option in the **Auto Discover Mode** option, System Manager displays the EventTracker – System Manager message box.

Figure 173 Delete Group – message box

EventTracker - System Manager
Please note that in 'Auto Discover' mode it is recommended not to delete groups based on domains as they are created automatically.
OK

7 Click **OK** to continue deleting the Groups.

Changing System Type

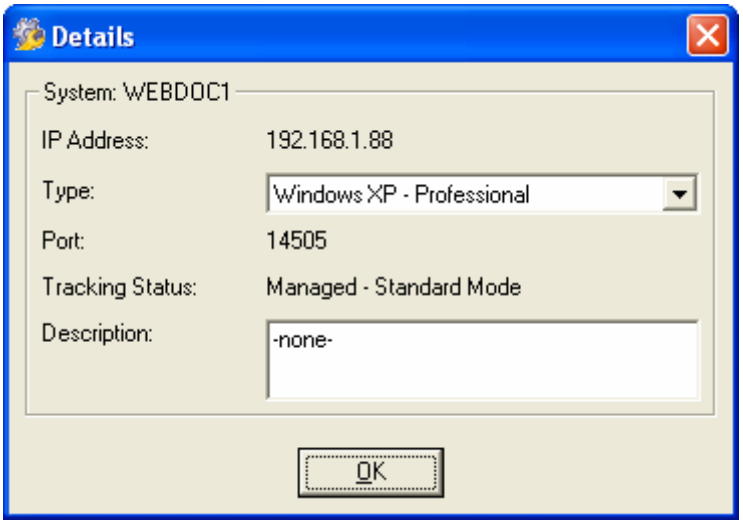
This option helps to change the type of systems.

To change system type

1 Open the System Manager.

2 Double-click the system that you want to change the system type.

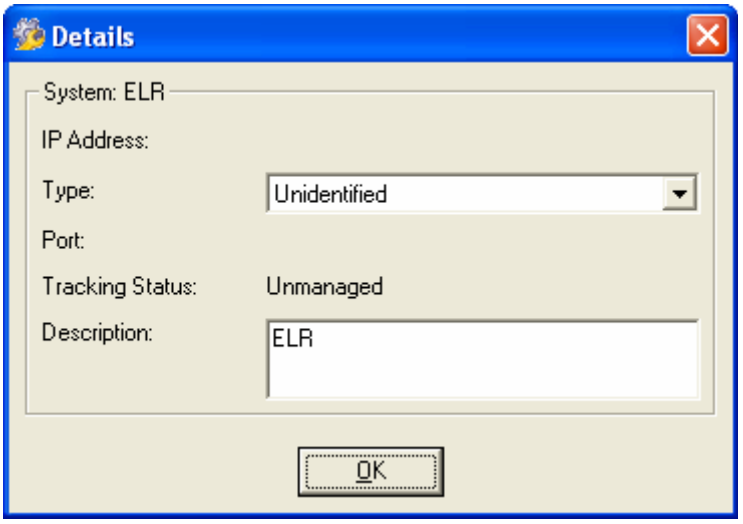
Figure 174 System Details



System Manager displays the identified O/S type in the Type drop-down list

.

Figure 175 System Details



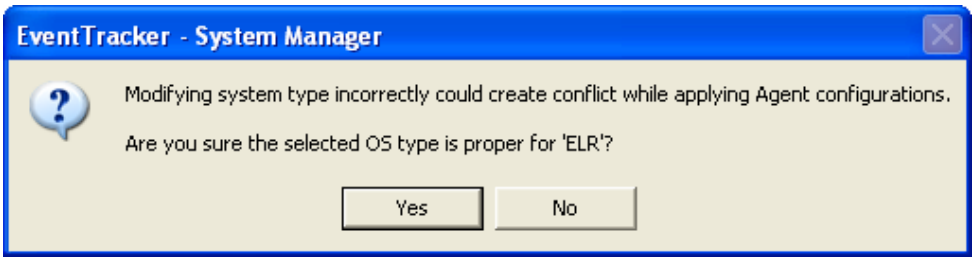
If the System Manager could not identify the O/S type, then it will display "Unidentified" in the Type drop-down list.

3 Select an O/S type from the **Type** drop-down list and then click **OK**.

System Manager displays the warning message.

.

Figure 176 System Details


EventTracker - System Manager
Modifying system type incorrectly could create conflict while applying Agent configurations.
Are you sure the selected OS type is proper for 'ELR'?
Yes
No

4 Click **Yes** to change the type.

5 Refresh the System Manager.

Chapter 8
Managing Windows Agents

In this chapter, you will learn about:

- Deploying Agents
- Agent Configuration
- Agent Management Tool
- Deploying Agents in Command Line Mode

Agent for Windows Systems

As part of the Windows event log management infrastructure, a configurable, high performance, tiny footprint executable (agent) can be deployed to run locally on the managed machine. The agent is usually remotely deployed directly from the System Manager application which is part of EventTracker.

In addition to sending entries from the Event Log, this agent offers many useful features including monitoring application log files, threshold events on CPU/memory/disk utilization, application start/stop, software install/uninstall; service start/stop & runaway processes and monitor TCP/UDP network activities. It can send events with guaranteed delivery (TCP), offers a sophisticated set of filters to limit event transmittal and performs automatic backup and clearing of the Windows Event Log (XP and 2003).

This "smart" agent offers significantly greater capability over manual log monitoring.

Pros

- Filters are applied locally - This minimizes network traffic as uninteresting events can be discarded with no further drain on resources.
- Local agent survives in the face of network failure - If the Guaranteed Delivery Mode (GED) is used, events are cached and recovered when network recovers.
- Real time notification – The agent immediately forwards new local event log entries to the Console. Critical events relating to security, uptime etc usually requires immediate alerts.
- Performance monitoring – The agent is capable of detecting excessive CPU, disk or memory usage and reporting if when user defined thresholds are detected.
- Application monitoring – The agent is capable of detecting and reporting the start/stop of applications. This can be used to comply with licensing requirements or for usage tracking.
- Native backup of event logs – The agent is capable of detecting when the event log is full, backing up the native .evt file to a configured location and resetting the log. Some installations require the original files (XP and 2003).
- Software install/removal monitoring – The agent can detect and report the installation or removal of software from the target machine.
- Non-domain topology – The agent needs only a TCP/IP network to communicate with the Console. In particular the Console is not required to be in the same Windows (Active Directory or NT) domain as the agent.
- Encrypted traffic between Agent and Console – IPSec techniques can be applied to all traffic between agent and Console for highest security.

- Service monitoring – The agent is capable of detecting, reporting and restarting failed services.
- Monitoring external log files – Many applications write a separate log file (e.g. IIS, Antivirus, Oracle etc). New matching entries in such log files can be detected and reported by the agent.
- Host based intrusion detection – The agent can detect and report network activity. This is useful as for capacity analysis or intrusion detection.

Cons

- The agent must be installed and configured on the target machine - This requires planning. Managing product upgrades must also be considered. Deployment and configuration can be done from the Console to minimize this effort.
- Possible interaction effects with other software – Since the agent is an EXE and does get installed on the target machine, there is always a finite probability of negative interaction effects with other software. The product has operated at many customers in many different environments for many years – so this highly unlikely.
- Agent consumes local resources – The agent, like any application uses some amount of system resources on the target. The EventTracker agent is highly optimized to absolutely minimize resource usage.

Deploying Agents

Pre-installation Procedures

- You MUST have Local Admin privileges on the remote systems where you want to install the Agents.
- You can also install Agents with Domain Admin privileges.
- Make sure that the systems that you are selecting to monitor are accessible through the network, have disks that are shared for the Admin, and have disk space up to 5MB that can be used by the Windows Agent.
- If the remote system is accessed through a slow line, the install may take time and it is recommended that you plan accordingly.

Installing Windows Agents

This option enables you to install Windows Agents in Standard mode.

To install agents in Standard mode

1. Open the System Manager.
2. Click the **Options** menu and select the **Add System** option

   (OR)

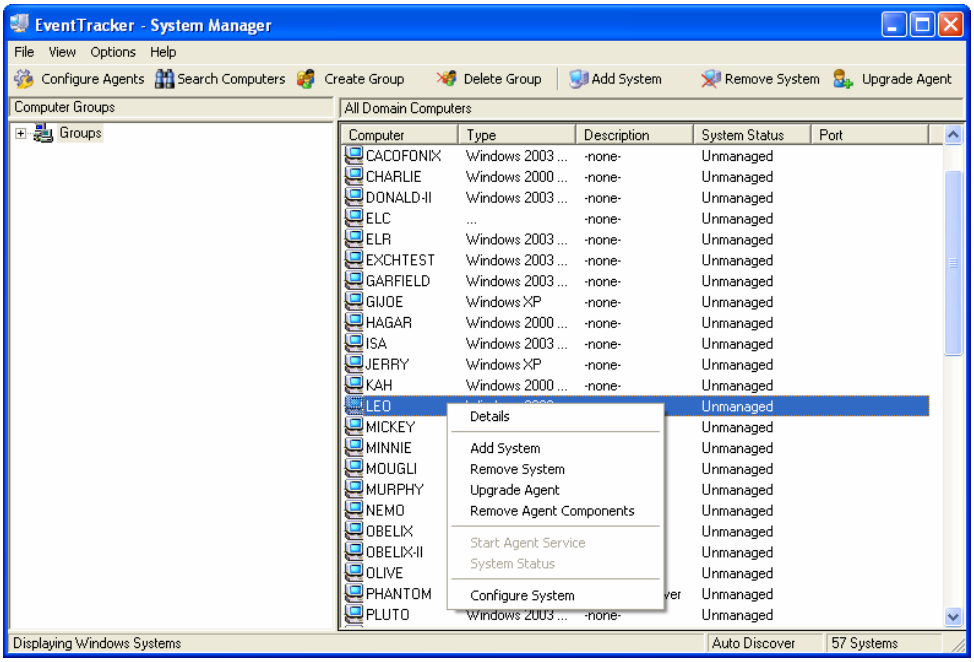
   Click **Add System** on the toolbar.

(OR)

Right-click the system where you want to install the agent.

System Manager displays the shortcut menu.

Figure 177 Add System



From the shortcut menu, choose the **Add System** option.

System Manager displays the Add Agent window.

Figure 178 Add Agent

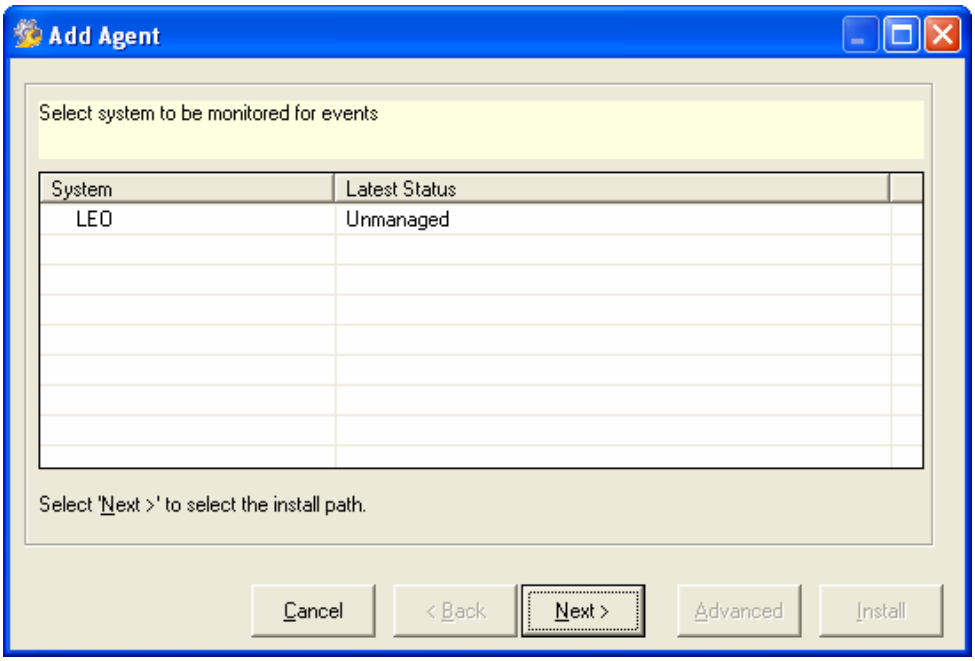


Figure 179 Add Agent

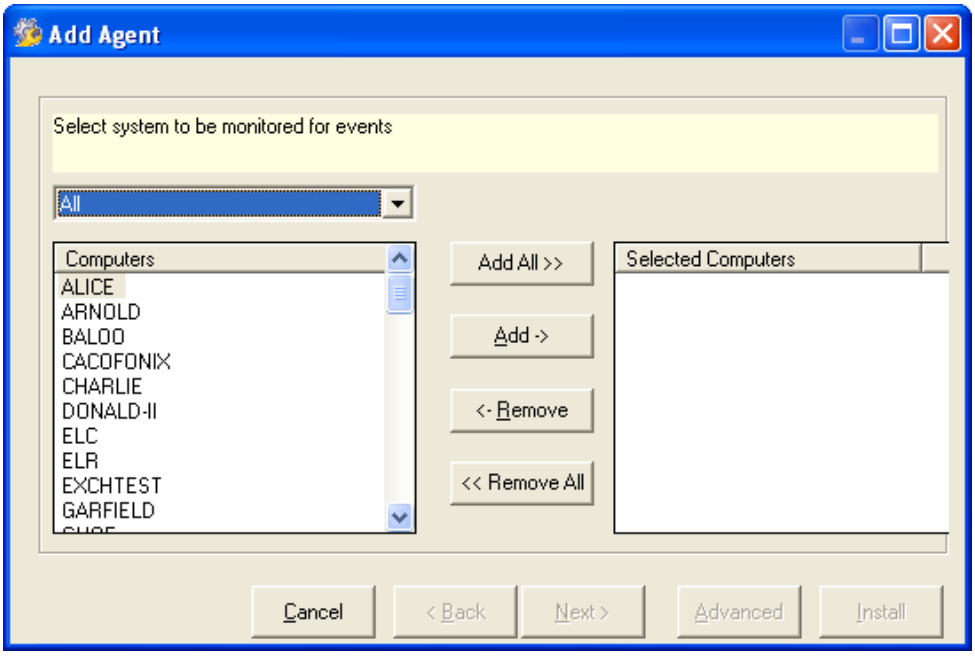


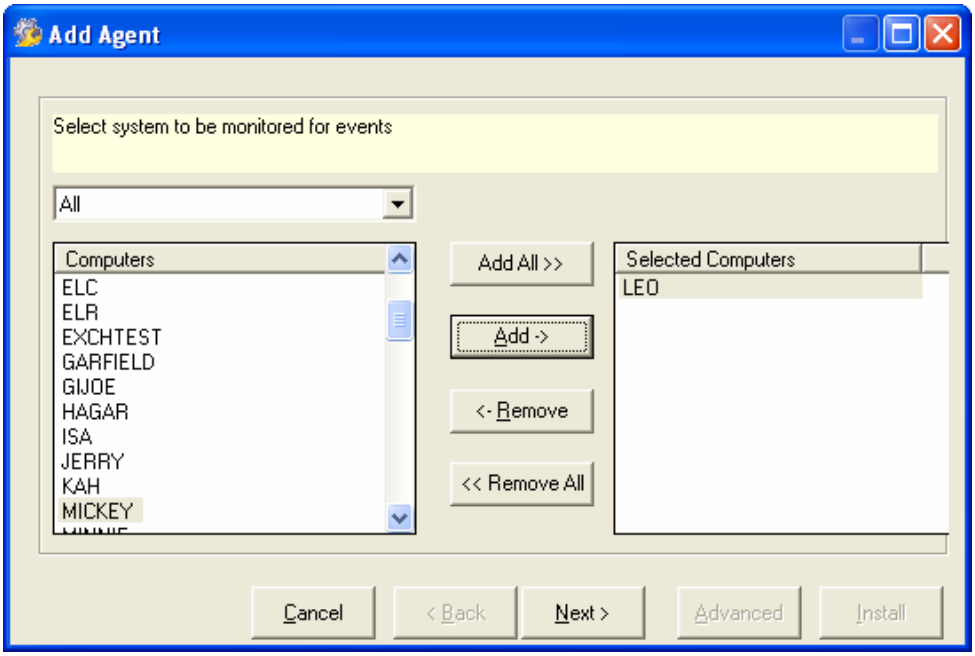
Table 35

Field	Description
Group	Select a group from the drop-down list.
Computers	Select a computer on which you want to install the Agent. Click **Add->**. The selected computer is added to the Selected Computers list. Click **Add All >>** to install the Agents on all the computers in the selected group.
Selected Computers	Select a computer and then click **<-Remove.** The selected computer is removed from the list. Click **<< Remove All** to remove all the computers from the list.

3 Select the systems.

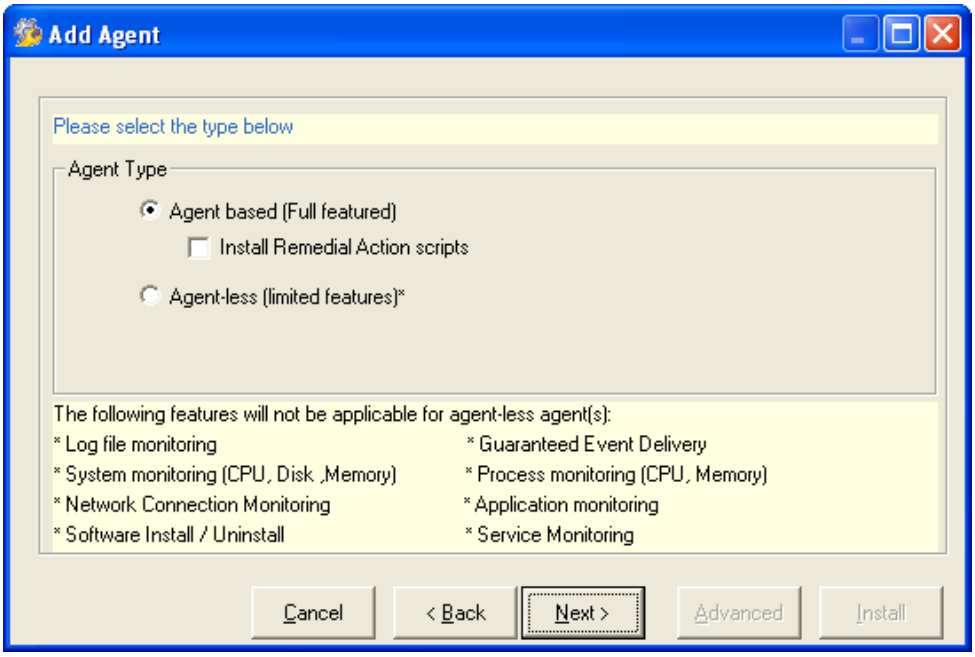
4 Click **Next>**.

Figure 180 Add Agent



5 Click **Next>**.

Figure 181 Add Agent – Agent Type

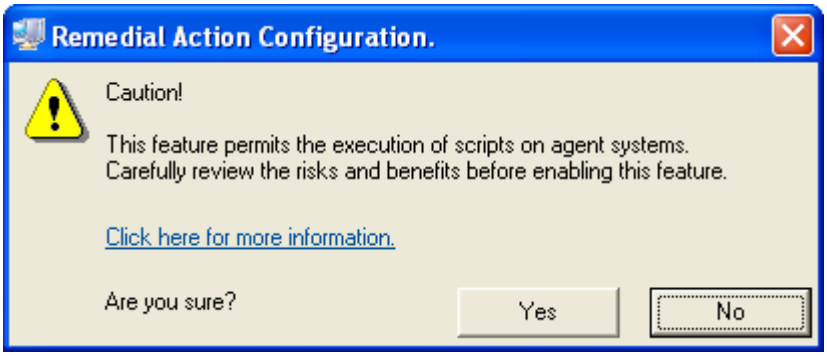


6 Select the **Agent based (Full featured)** option

7 Select the **Install Remedial Action scripts** check box to install the scripts in the EventTracker install directory, typically (…\Program Files\Prism Microsystems\EventTracker\Agent\Script).

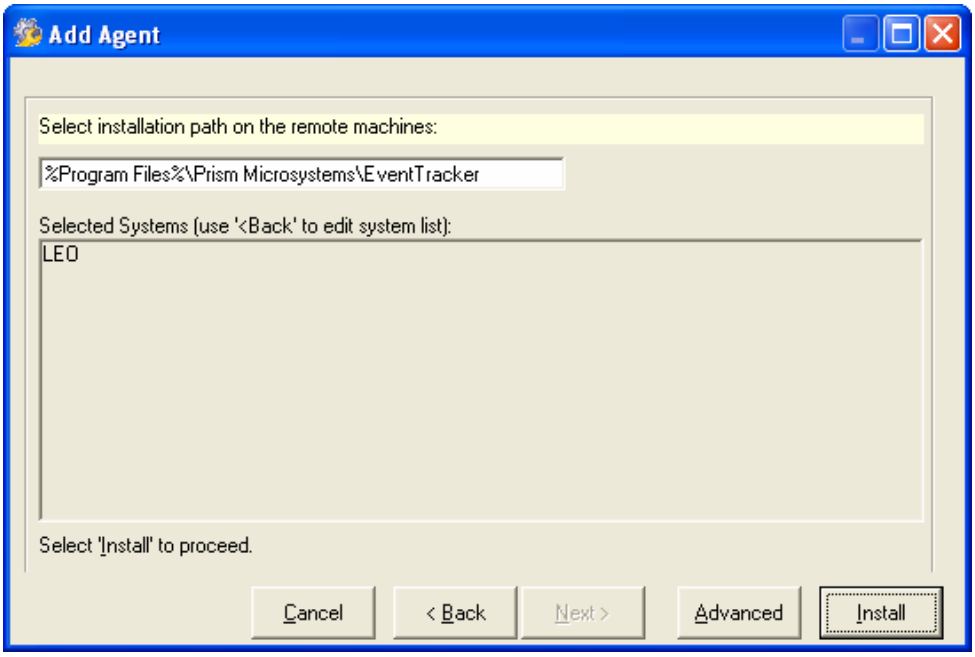
System Manager displays the Caution message box. Click **Yes** to install scripts.

Figure 182 Remedial Action Configuration


Remedial Action Configuration.
Caution!
This feature permits the execution of scripts on agent systems.
Carefully review the risks and benefits before enabling this feature.
Click here for more information.
Are you sure?
Yes
No

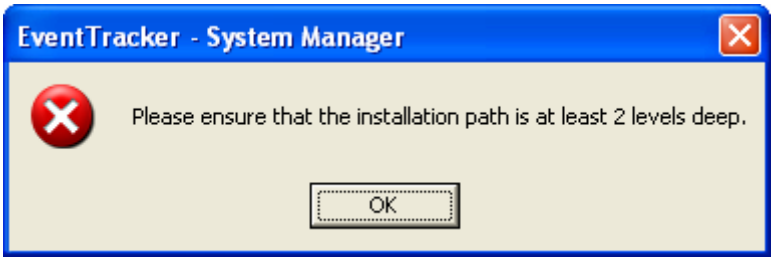
8 Click **Next>**.

Figure 183 Add Agent – Installation path



9 To install the agent in a different drive apart from the default one, type the installation path in the **Select installation path on the remote machines** field. System Manager displays the EventTracker - System Manager message box if the typed path is not of recommended levels deep.

Figure 184 System Manager message box



Note

To set a more specific configuration, click **Advanced** (OR) click **Install** to install the Agent.

10 Click **Advanced**.

Figure 185 Add Agent – Apply default configuration

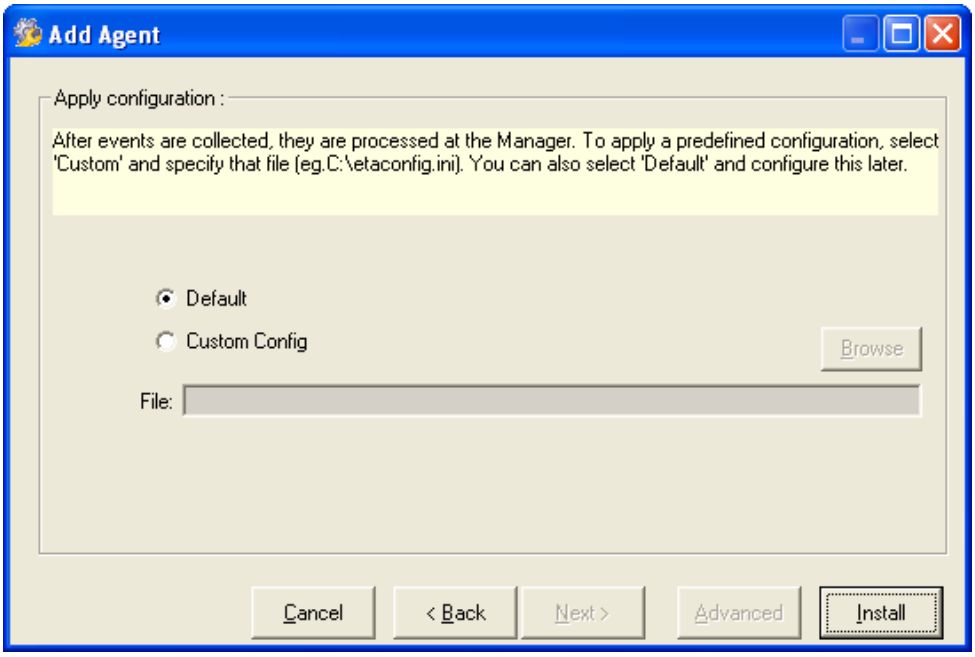
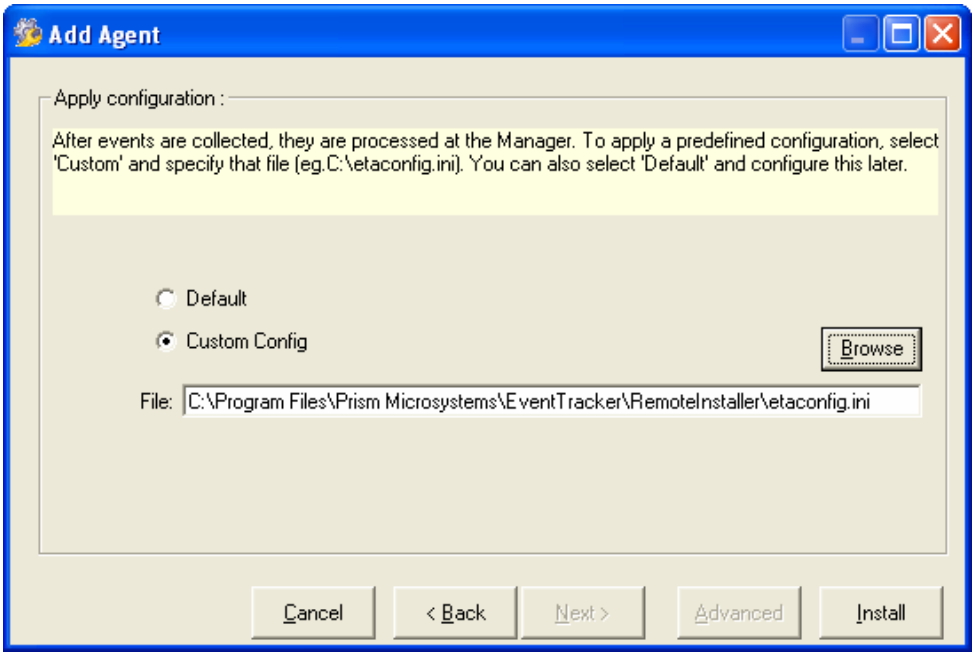

Add Agent
Apply configuration :
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify that file (eg.C:\etaconfig.ini). You can also select 'Default' and configure this later.
Default
Custom Config
Browse
File:
Cancel
< Back
Next >
Advanced
Install

Table 36

Field	Description
Default	Select this option to set the default agent configuration. The default configuration will track all events.
Custom Config	Select this option to apply a different configuration. The File field is enabled. Click **Browse**, navigate and select the file. The file extension should be in the EventTracker Agent `.ini` format and would be a previously saved configuration file.

11 Click the appropriate agent configuration settings.

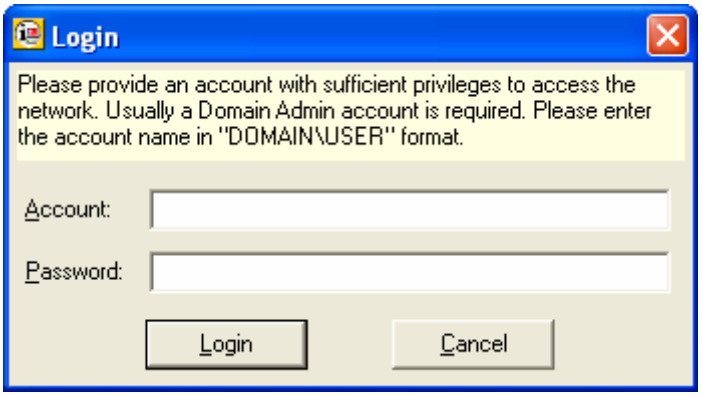
Figure 186 Add Agent – Apply custom configuration


Add Agent
Apply configuration :
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify that file (eg.C:\etaconfig.ini). You can also select 'Default' and configure this later.
Default
Custom Config
Browse
File:
C:\Program Files\Prism Microsystems\EventTracker\RemoteInstaller\etaconfig.ini
Cancel
< Back
Next >
Advanced
Install

12 Click **Install**.

System Manager displays the Login dialog box.

Figure 187 Add Agent – Login

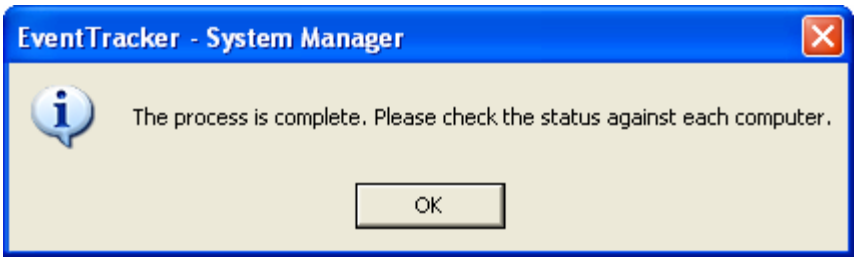

Login
Please provide an account with sufficient privileges to access the network. Usually a Domain Admin account is required. Please enter the account name in "DOMAIN\USER" format.
Account:
Password:
Login
Cancel

13 Type valid user credentials and then click **Login**.

System Manager starts installing the Agent and displays the progress bar.

After installing the Agent, System Manager displays the EventTracker – System Manager message box.

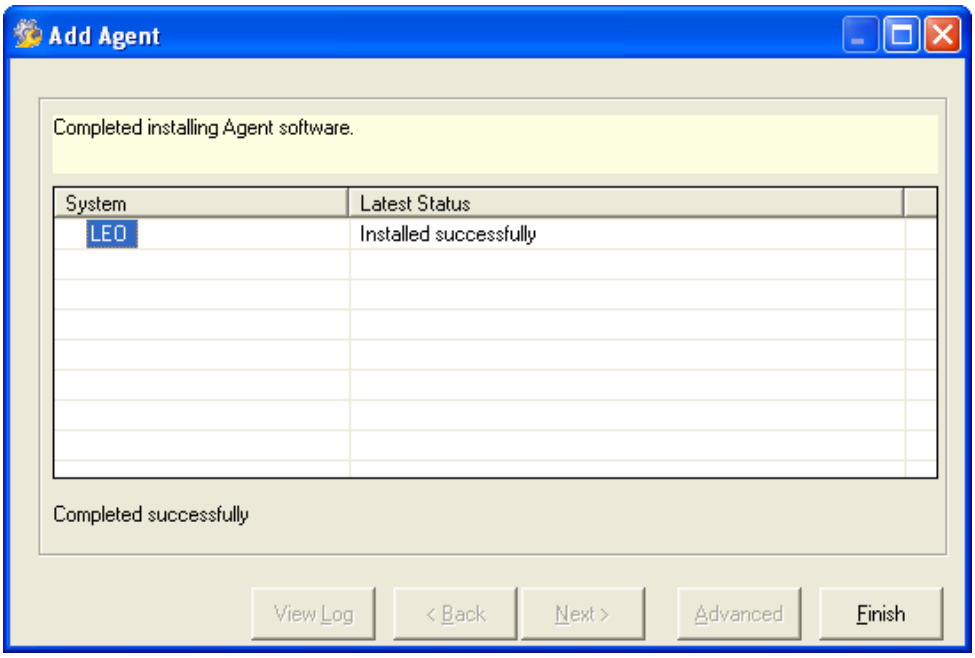
Figure 188 System Manager – message box



14 Click **OK**.

System Manager displays the successful installation message.

Figure 189 Add Agent – Successful installation message

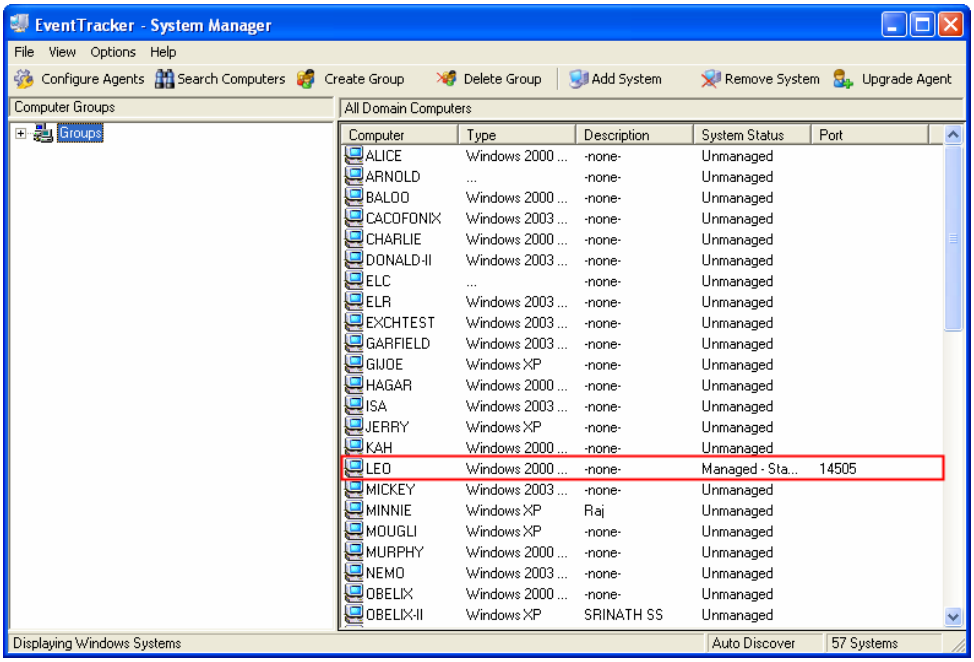


15 Click **Finish**.

16 To refresh the System Manager, click the **View** menu and select the **Refresh** option or press **F5** on your keyboard.

System Manager displays the newly added system.

Figure 190 System Manager - newly added system


EventTracker - System Manager
File View Options Help
Configure Agents
Search Computers
Create Group
Delete Group
Add System
Remove System
Upgrade Agent
Computer Groups
Groups
All Domain Computers
Computer
Type
Description
System Status
Port
ALICE Windows 2000 ... -none- Unmanaged
ARNOLD ... -none- Unmanaged
BALOO Windows 2000 ... -none- Unmanaged
CACOFONIX Windows 2003 ... -none- Unmanaged
CHARLIE Windows 2000 ... -none- Unmanaged
DONALD-II Windows 2003 ... -none- Unmanaged
ELC ... -none- Unmanaged
ELR Windows 2003 ... -none- Unmanaged
EXCHTEST Windows 2003 ... -none- Unmanaged
GARFIELD Windows 2003 ... -none- Unmanaged
GIJOE Windows XP -none- Unmanaged
HAGAR Windows 2000 ... -none- Unmanaged
ISA Windows 2003 ... -none- Unmanaged
JERRY Windows XP -none- Unmanaged
KAH Windows 2000 ... -none- Unmanaged
LEO Windows 2000 ... -none- Managed - Sta... 14505
MICKEY Windows 2003 ... -none- Unmanaged
MINNIE Windows XP Raj Unmanaged
MOUGLI Windows XP -none- Unmanaged
MURPHY Windows 2000 ... -none- Unmanaged
NEMO Windows 2003 ... -none- Unmanaged
OBELIX Windows 2000 ... -none- Unmanaged
OBELIX-II Windows XP SRINATH SS Unmanaged
Displaying Windows Systems
Auto Discover
57 Systems

Uninstalling Windows Agents

This option enables you to uninstall Windows Agent from the remote computer.

To uninstall Windows Agents

1. Open the System Manager.
2. Select the **Options** menu and select the **Remove System** option

   (OR)

   Click **Remove System** on the toolbar.

   (OR)

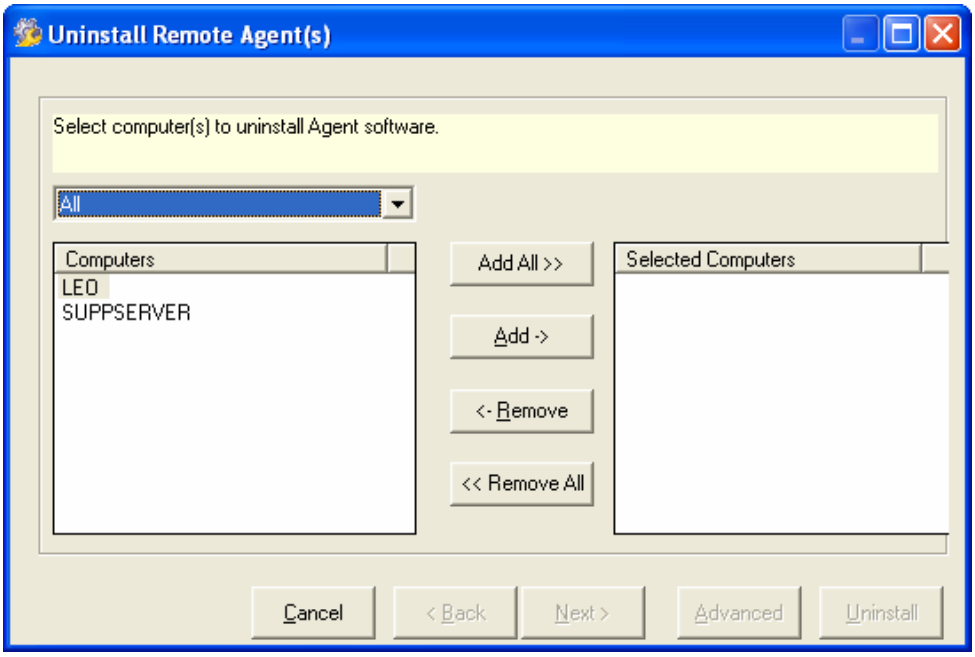
   Right-click the system from where you want to uninstall the agent.

   System Manager displays the shortcut menu.

   From the shortcut menu, choose the **Remove System** option.

   System Manager displays the Uninstall Remote Agent(s) window.

Figure 191 Uninstall Remote Agent(s) – Computer selection

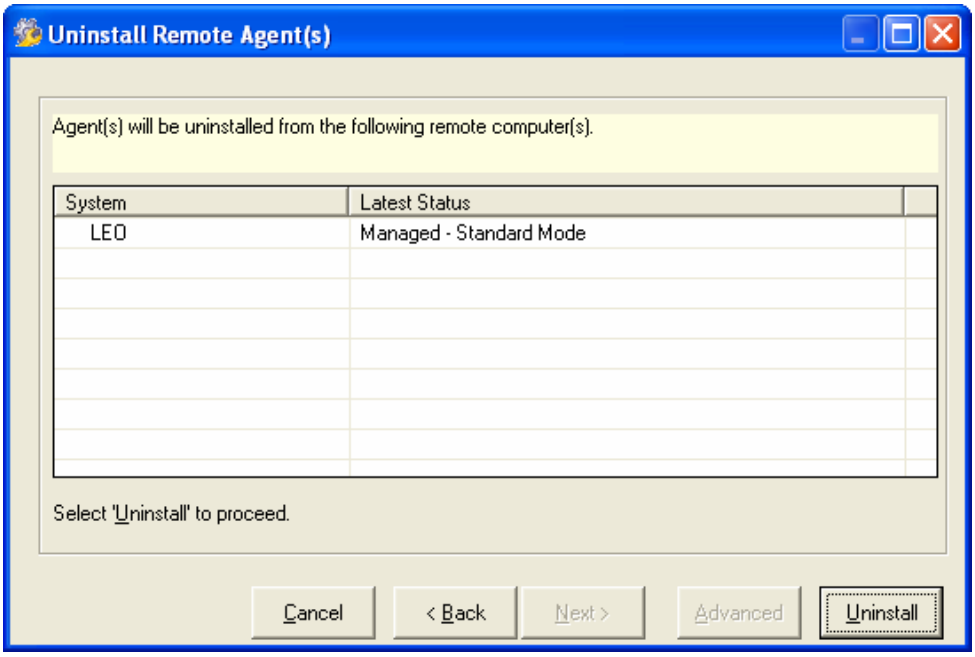


For field descriptions, refer Figure 268 Add System window on page 184.

3 Select the computer.

4 Click **Next>**.

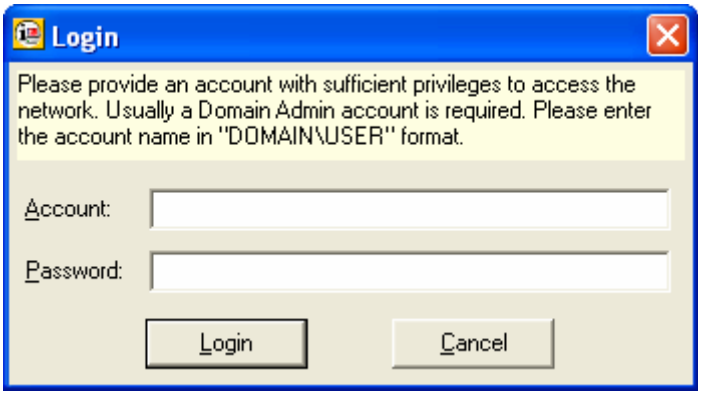
Figure 192 Uninstall Remote Agent(s)



5 Click **Uninstall**.

System Manager displays the Login dialog box.

Figure 193 Uninstall Remote Agent(s) – Login

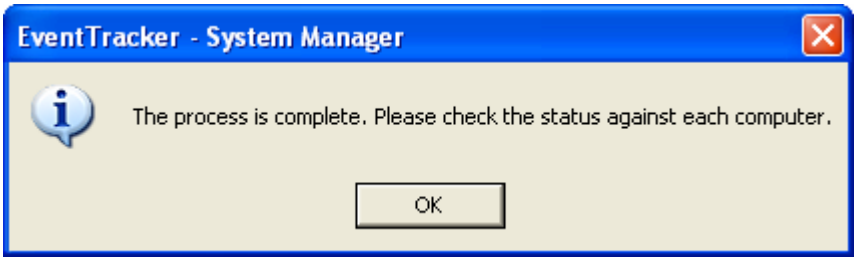

Login
Please provide an account with sufficient privileges to access the network. Usually a Domain Admin account is required. Please enter the account name in "DOMAIN\USER" format.
Account:
Password:
Login
Cancel

6 Type valid user credentials and then click **Login**.

System Manager starts uninstalling the Agent and displays the progress bar.

After successfully uninstalling the Agent, System Manager displays the EventTracker – System Manager message box.

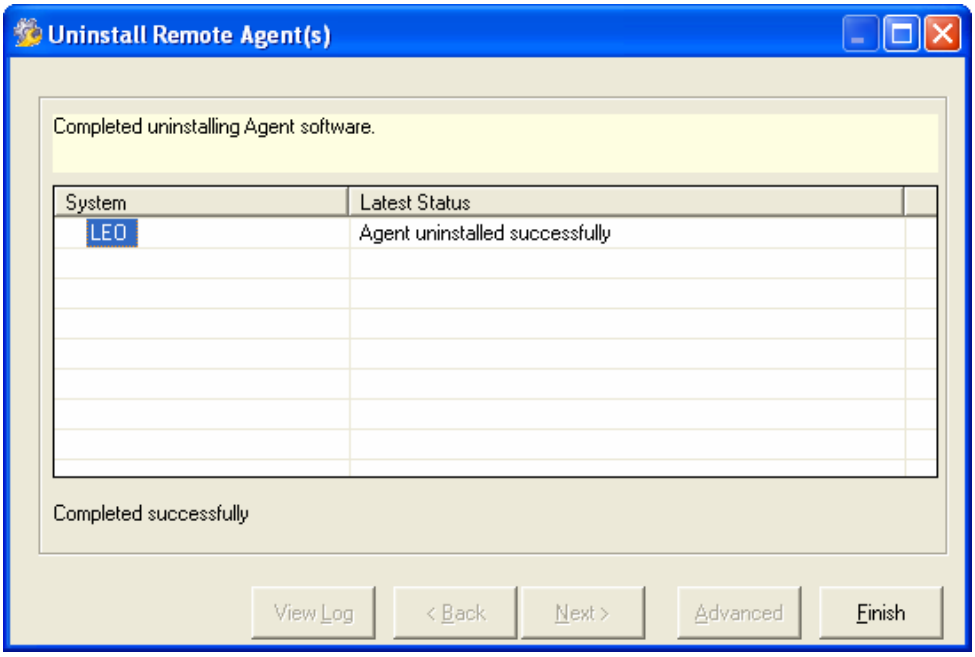
Figure 194 Uninstalling Agent – message box



7 Click **OK**.

System Manager displays the successful uninstallation message.

Figure 195 Uninstall Remote Agent(s) – Successful uninstall message



8 Click **Finish**.

Upgrading Windows Agents

This option enables you to upgrade Windows Agents that are within the domain by selecting "Windows Domain Network" option and "Upgrade over IP" option that are outside the domain.

To upgrade Agents

1 Open the System Manager.

2 Click the **Options** menu and select the **Upgrade Agent** option

(OR)

Click **Upgrade Agent** on the toolbar.

(OR)

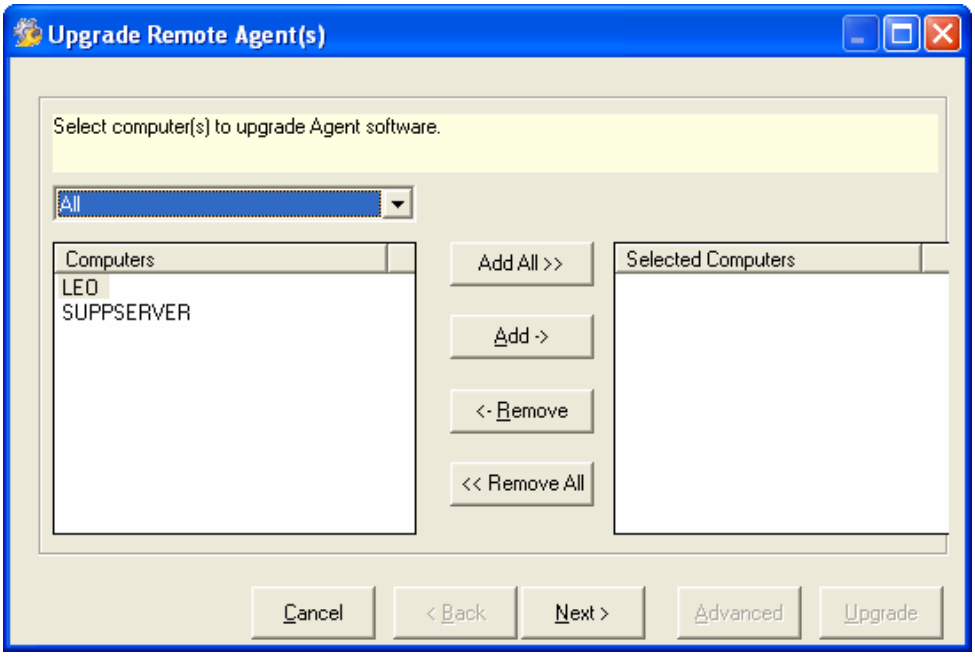
Right-click the system to upgrade the agent installed in it.

System Manager displays the shortcut menu.

From the shortcut menu, choose the **Upgrade Agent** option.

System Manager displays the Upgrade Remote Agent(s) window.

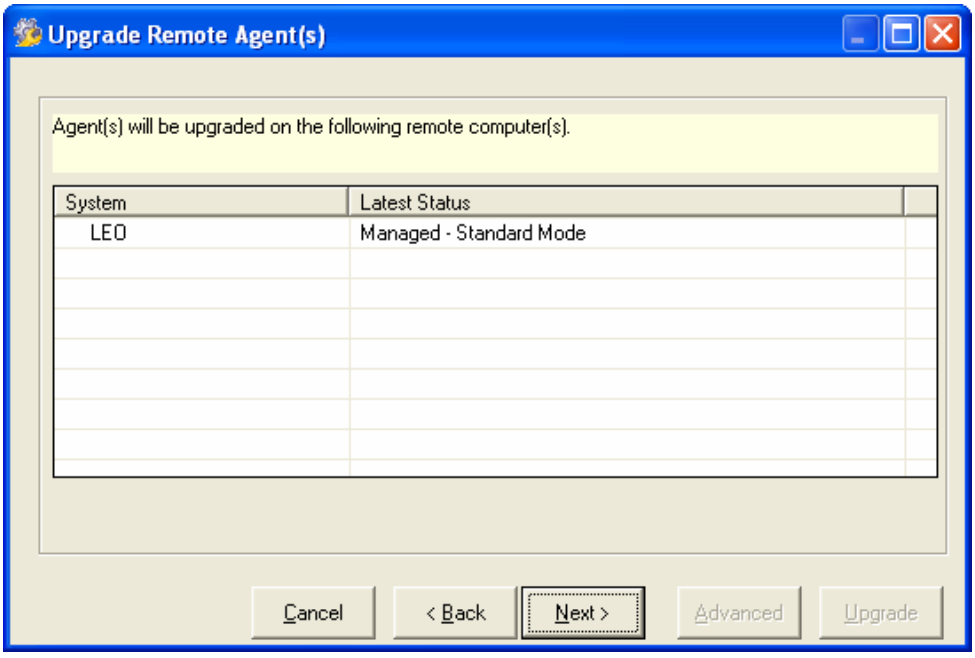
Figure 196 Upgrade Remote Agent(s)



3 Select the computer for which you want to upgrade the Agent.

4 Click **Next**>.

Figure 197 Upgrade Remote Agent(s)



5 Click **Next**>.

Figure 198 Upgrade Remote Agent(s)

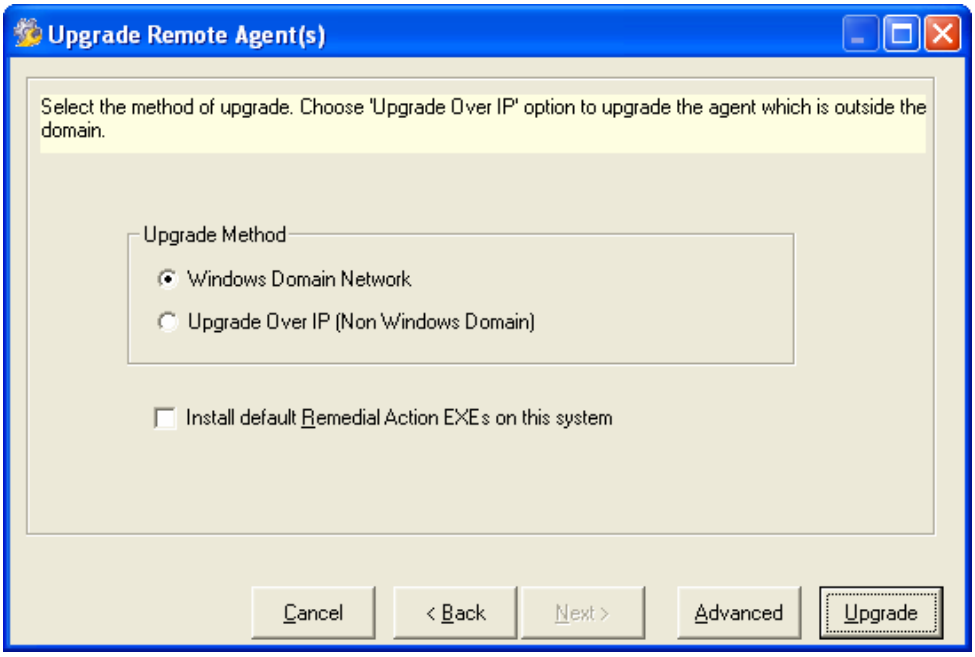

Upgrade Remote Agent(s)
Select the method of upgrade. Choose 'Upgrade Over IP' option to upgrade the agent which is outside the domain.
Upgrade Method
Windows Domain Network
Upgrade Over IP (Non Windows Domain)
Install default Remedial Action EXEs on this system
Cancel
< Back
Next >
Advanced
Upgrade

Table 37

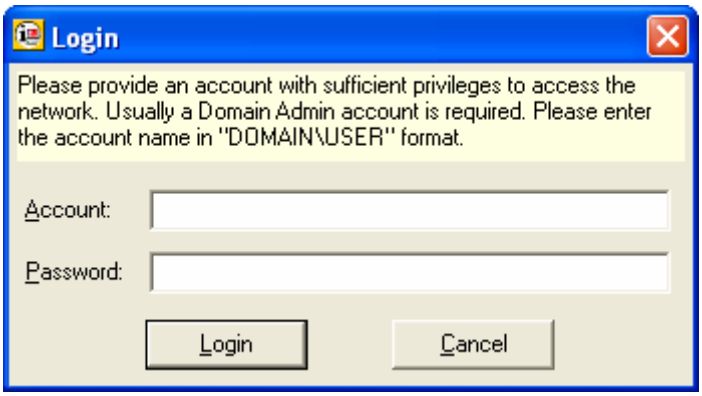
Field	Description
Upgrade Method	
Windows Domain Network	Select this option if all systems to be upgraded can be reached over the Windows Network and you have administrative privileges on all these systems.
Upgrade Over IP (Non Windows Domain)	Select this option if all systems to be upgraded can be reached only via IP and not by the Microsoft Network.
Install default Remedial Action EXEs on this system	Select this check box to install remedial executables on this system.

6 Click the appropriate **Upgrade Method**.

7 Click **Upgrade**.

System Manager displays the Login dialog box.

Figure 199 Upgrade Agent(s) – Login

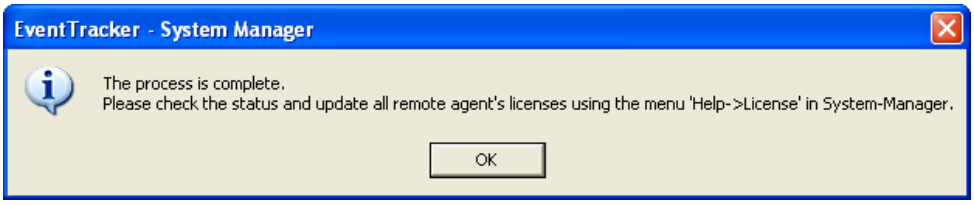

Login
Please provide an account with sufficient privileges to access the network. Usually a Domain Admin account is required. Please enter the account name in "DOMAIN\USER" format.
Account:
Password:
Login
Cancel

8 Type valid user credentials and then click **Login**.

System Manager starts upgrading the Agent and displays the progress bar.

After upgrading the Agent, System Manager displays the EventTracker – System Manager message box.

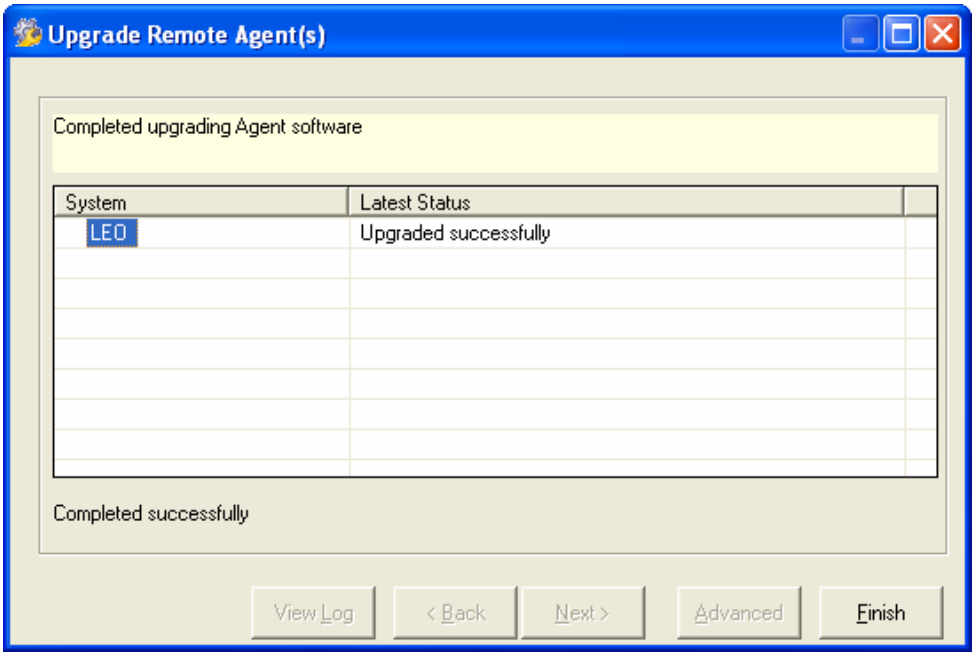
Figure 200 Upgrade Agent(s) – message box


EventTracker - System Manager
The process is complete.
Please check the status and update all remote agent's licenses using the menu 'Help->License' in System-Manager.
OK

9 Click **OK**.

System Manager displays the successful upgrade message.

Figure 201 Upgrade Remote Agent(s) – Successful upgrade message



10 Click **Finish**.

Removing Windows Agent Components

This option enables you to remove Windows Agent components

To remove Windows Agent components

1 Open the System Manager.

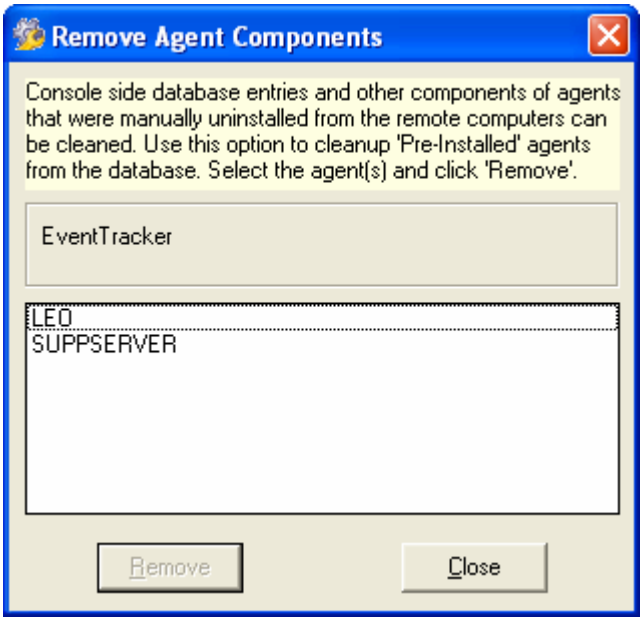
2 Click the **Options** menu and select the **Remove Agent Components** option.

(OR)

Right-click any of the systems in the right pane.

System Manager displays the Remove Agent Components dialog box.

Figure 202 Remove Agent Components

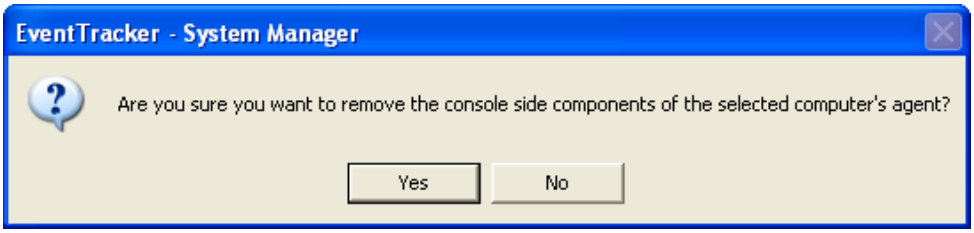

Remove Agent Components
Console side database entries and other components of agents that were manually uninstalled from the remote computers can be cleaned. Use this option to cleanup 'Pre-Installed' agents from the database. Select the agent(s) and click 'Remove'.
EventTracker
LEO
SUPPSERVER
Remove
Close

3 Select the computer for which you want to remove the Agent from the list.

4 Click **Remove**.

System Manager displays the EventTracker – System Manager confirmation message box.

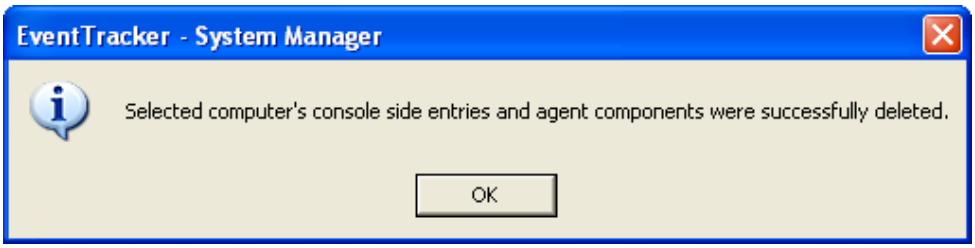
Figure 203 System Manager message box


EventTracker - System Manager
Are you sure you want to remove the console side components of the selected computer's agent?
Yes
No

5 Click **Yes**.

System Manager displays the EventTracker – System Manager message box.

Figure 204 System Manager message box


EventTracker - System Manager
Selected computer's console side entries and agent components were successfully deleted.
OK

6 Click **OK**.

7 Click **Close** on the Remove Client Components dialog box.

Switching Windows Agent Modes

This option enables you to switch Windows Agent mode from Standard mode to High Performance mode and vice versa. This can be done either via the Microsoft Network or over the IP Network.

To switch Windows Agent modes

1 Open the System Manager.

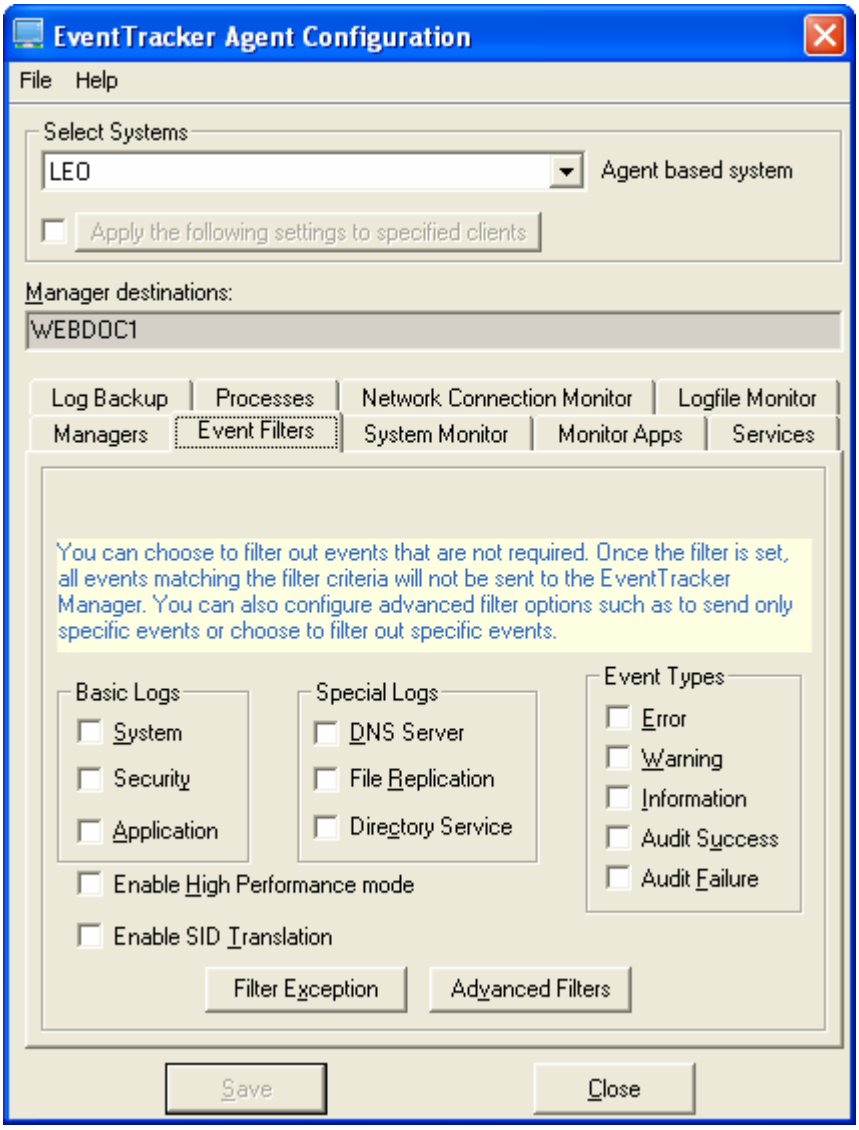
2 Click the **Options** menu and select the **Configure System** option

System Manager displays the Agent Configuration window.

3 Select the system that you want to switch the Agent mode from the **Select Systems** drop-down list and then click **Event Filters** tab

System Manager displays the Agent Configuration window.

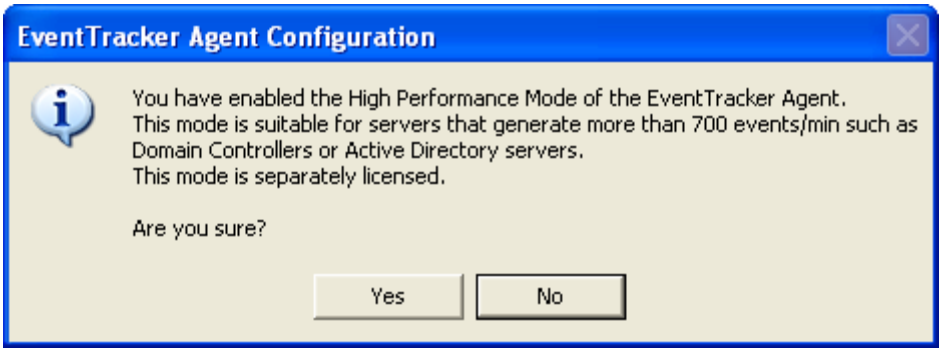
Figure 205
EventTracker Agent Configuration window



4 Select the **Enable High Performance mode** check box.

System Manager displays the EventTracker Agent Configuration message box.

Figure 206 EventTracker Agent Configuration message box


EventTracker Agent Configuration
You have enabled the High Performance Mode of the EventTracker Agent.
This mode is suitable for servers that generate more than 700 events/min such as Domain Controllers or Active Directory servers.
This mode is separately licensed.
Are you sure?
Yes
No

5 Click **Yes**.

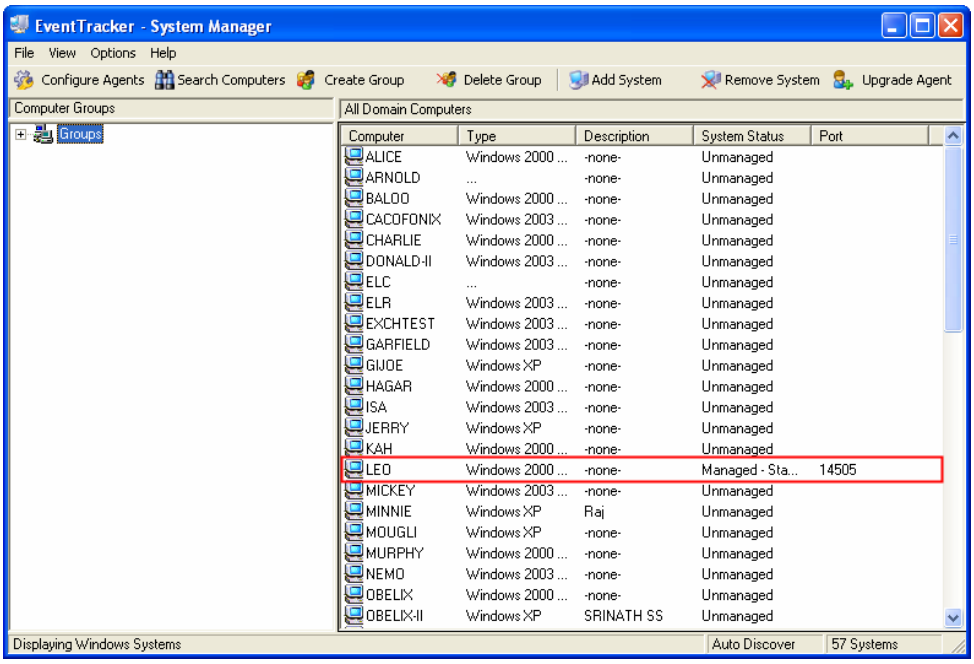
6 Click **Save**.

7 Click **Close** on the Agent Configuration window.

8 To refresh the System Manager, select the **View** menu and select the **Refresh** option or press **F5** on your keyboard.

System Manager displays the upgraded system.

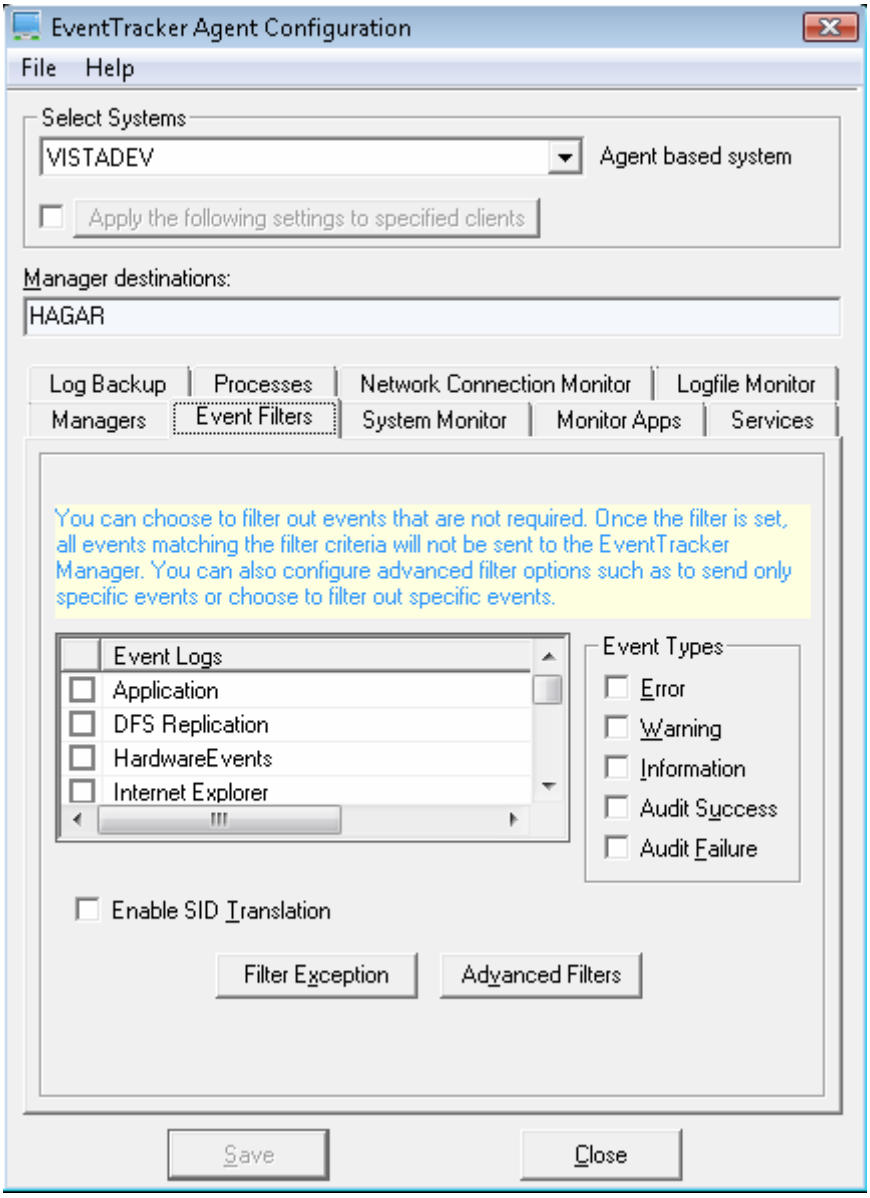
Figure 207 System Manager console with newly added system


EventTracker - System Manager
File View Options Help
Configure Agents Search Computers Create Group Delete Group Add System Remove System Upgrade Agent
Computer Groups
Groups
All Domain Computers
Computer Type Description System Status Port
ALICE Windows 2000 ... -none- Unmanaged
ARNOLD ... -none- Unmanaged
BALOO Windows 2000 ... -none- Unmanaged
CACOFONIX Windows 2003 ... -none- Unmanaged
CHARLIE Windows 2000 ... -none- Unmanaged
DONALD-II Windows 2003 ... -none- Unmanaged
ELC ... -none- Unmanaged
ELR Windows 2003 ... -none- Unmanaged
EXCHTEST Windows 2003 ... -none- Unmanaged
GARFIELD Windows 2003 ... -none- Unmanaged
GIJOE Windows XP -none- Unmanaged
HAGAR Windows 2000 ... -none- Unmanaged
ISA Windows 2003 ... -none- Unmanaged
JERRY Windows XP -none- Unmanaged
KAH Windows 2000 ... -none- Unmanaged
LEO Windows 2000 ... -none- Managed - Sta... 14505
MICKEY Windows 2003 ... -none- Unmanaged
MINNIE Windows XP Raj Unmanaged
MOUGLI Windows XP -none- Unmanaged
MURPHY Windows 2000 ... -none- Unmanaged
NEMO Windows 2003 ... -none- Unmanaged
OBELIX Windows 2000 ... -none- Unmanaged
OBELIX-II Windows XP SRINATH SS Unmanaged
Displaying Windows Systems
Auto Discover
57 Systems

Note

This feature is not applicable for Vista Agent.

Figure 208
EventTracker Agent Configuration window – Vista Agent



Viewing Agent Status

This option enables you to view the system health status.

To view agent status

1. Open the System Manager.
2. Select the system in the right pane.
3. Click the **View** menu and select the **System Status** option.

   (OR)

   Right-click the system that you want to view the status.

   System Manager displays the shortcut menu.

   From the shortcut menu, choose the **System Status** option.

   System Manager displays the system status in the Notepad.

Starting the Agent Service

This option enables you to restart the terminated remote client service.

To start the Agent service

1. Open the System Manager.
2. Select the system in the right pane.
3. Click the **Options** menu and select the **Start Client Service** option.

   (OR)

   Right-click the system that you want to start the client service.

   System Manager displays the shortcut menu.

   From the shortcut menu, choose the **Start Client Service** option.

   System Manager starts the client service and displays the message in the Notepad.

   If the client is already running, System Manager displays the Client status with a suitable message in the Notepad.

Editing Admin Account

This option enables you to change the Client Service Account credentials. This can be used only for Clients that can be reached by the Microsoft Domain Network and for which you have administrator privileges.

To the admin account

1. Open the System Manager.
2. Click the **Options** menu and select the **Agent Properties** option.

   System Manager displays the EventTracker Agent Properties window.

Figure 209 Client Properties – Account tab

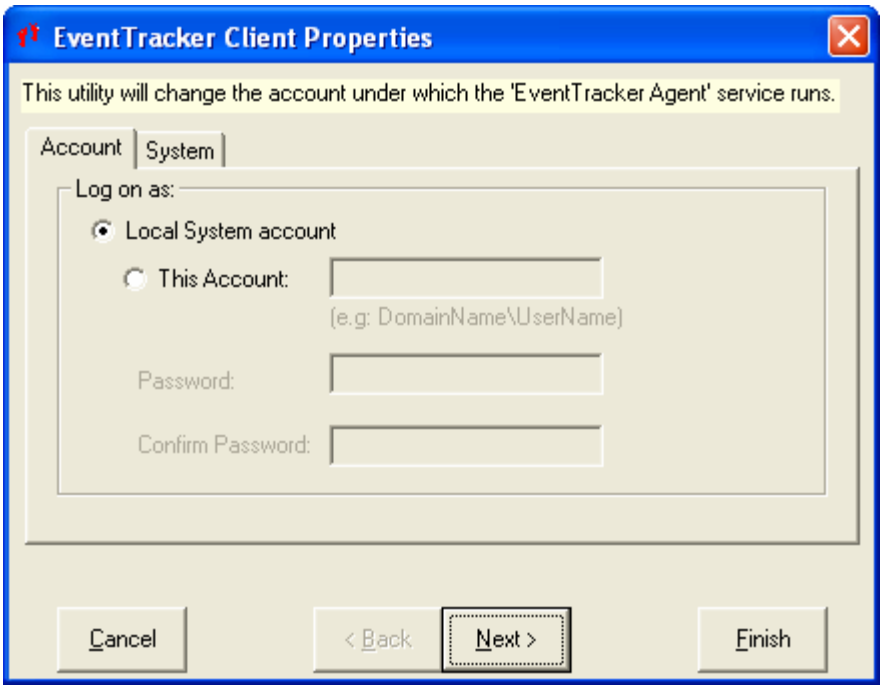


Table 38

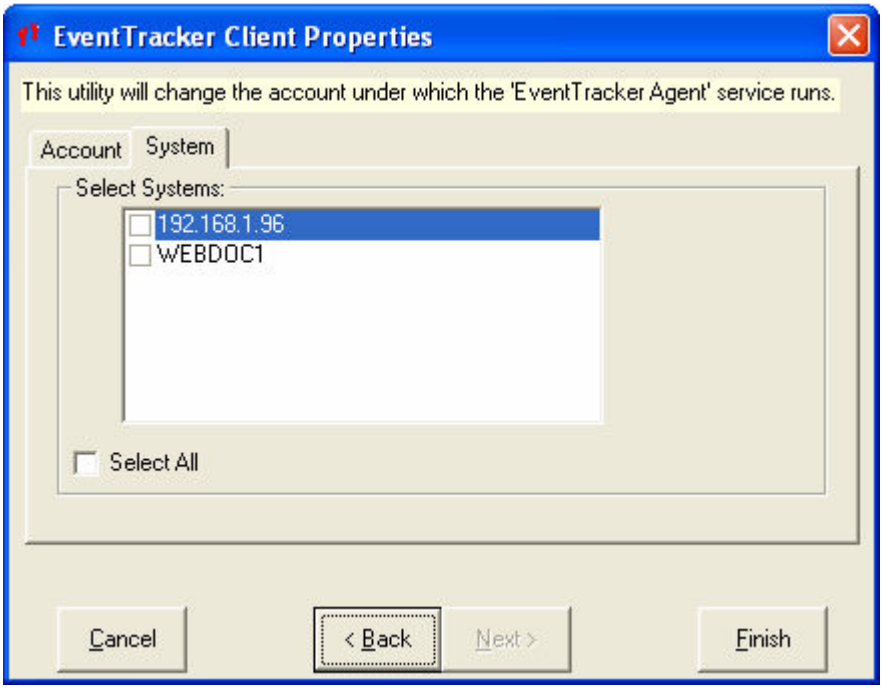
Field	Description
Local System account	Select this option to set the system account as the default logon for the service.
This Account	Select this option to change the logon account. This Account, Password and Confirm Password fields are enabled. Type the domain name and the user name in the This Account field. For example: CELEBRATE/administrator. Type the password in the Password field. Type the same password for confirmation in the Confirm Password field.

   Local System account is selected by default.

3. Select the This Account option and then enter valid user credentials.
4. Click **Next>**.

   System Manager displays the EventTracker Agent Properties window.

Figure 210 Client Properties – System tab



5 Select the system for which you want to apply the changes in the logon account

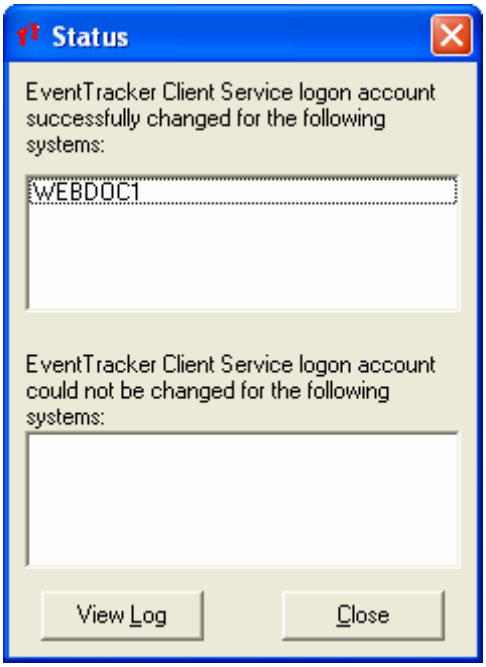
(OR)

Select the **Select All** check box to select all the systems in the list.

6 Click **Finish**.

System Manager displays the Status dialog box.

Figure 211 Client Service Logon Account - Status


Status
EventTracker Client Service logon account successfully changed for the following systems:
WEBDOC1
EventTracker Client Service logon account could not be changed for the following systems:
View Log
Close

7 Click **View Log** to view log.

System Manager displays the log information in the notepad.

8 Click **Close**.

Generating System Report

System Report helps you keep track of Managed and Unmanaged systems. Filter option is provided to view the ports used by Managed systems.

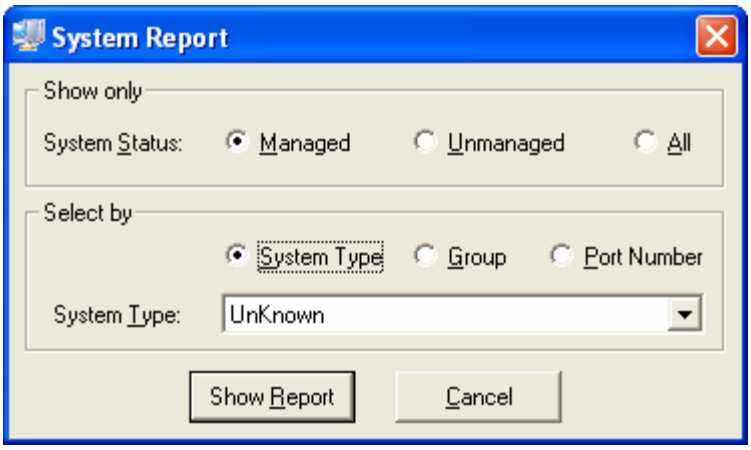
To generate system report

1 Open the System Manager.

2 Click the **View** menu and then select the **System Report** option.

System Manager displays the System Report console.

Figure 212 System Report



Note

EventTracker disables the **Port Number** option, if you select the **Unmanaged** option.

Managed System Report

This option helps you generate O/S wise, group wise and port wise report.

To generate system type wise report

1. Select the **Managed** option.
2. Select **System Type** option to view Managed systems by operation systems.
3. Select an O/S type from the **System Type** drop-down list.
4. Click **Show Report**.

Note

System Type **Unknown** represents non-Windows operating systems.

To generate group wise report

1. Select the **Managed** option.
2. Select the **Group** option to view Managed systems by group.
3. Select a group from the **Group Name** drop-down list. All monitored enterprise system groups are listed in this drop-down list.

4 Click **Show Report**.

To generate port wise report

1 Select the **Managed** option.

2 Select the **Port Number** option to view Managed systems by port. All configured ports are listed in this drop-down list.

3 Select a port from the **Port Number** drop-down list.

4 Click **Show Report**.

Unmanaged System Report

This option helps you generate O/S wise and group wise report.

To generate system type wise report

1 Select the **Managed** option.

2 Select **System Type** option to view Managed systems by operation systems.

3 Select an O/S type from the **System Type** drop-down list.

4 Click **Show Report**.

To generate group wise report

1 Select the **Managed** option.

2 Select the **Group** option to view Managed systems by group.

3 Select a group from the **Group Name** drop-down list.

4 Click **Show Report**.

All System Report

This option helps to generate O/S wise, group wise and port wise Managed / Unmanaged system report.

Vista Agent

Event Publishers in Windows Event Log

An event publisher creates an event and delivers it to an event log. An event publisher is typically an application, service, or driver. There can be multiple publishers for large

applications, and the publishers should be distinguished by the major components of an application.

Event Logs and Channels in Windows Event Log

A channel is a named stream of events that transports events from an event publisher to an event log file, where an event consumer can get an event. Event channels are intended for specific audiences and have different types for each audience. While most channels are tied to specific event publishers (they are created when publishers are installed and deleted when publishers are uninstalled), there are a few channels that are independent from any event publisher. System Event Log channels and event logs, such as System, Application, and Security, are installed with the operating system and cannot be deleted.

A channel can be defined on any independent Event Tracing for Windows (ETW) session.

Such channels are not controlled by Windows Event Log, but by the ETW consumer that creates them. Channels defined by event publishers are identified by a name and should be based on the publisher name.

Event Consumers in Windows Event Log

Event consumers are entities that receive events from a computer. Windows Event Viewer (EventVwr.exe) is a event consumer that displays event information from a variety of specified event logs.

There are two types of Windows Event Log consumers:

Subscribers

Applications that receive event notifications as they are received by Windows Event Log.

Event log readers

Applications that query logged events.

For more details, log on to Microsoft Web site.

Prerequisites

Following are the mandatory settings you ought to do on Vista systems before you deploy Vista Agent.

1. By default, the Startup Type of Remote Registry is manual. Modify the Startup Type as Automatic and Start the service.
2. Enable File and Printer Sharing.
3. Turn on and enable Network Discovery.

4 To configure Vista agent remotely, on Vista system add port no 14506 TCP to Firewall Exceptions.

5 The user must be domain administrator, member of domain admin, or must be added to the local administrator group on the Vista system where the agent has to be deployed.

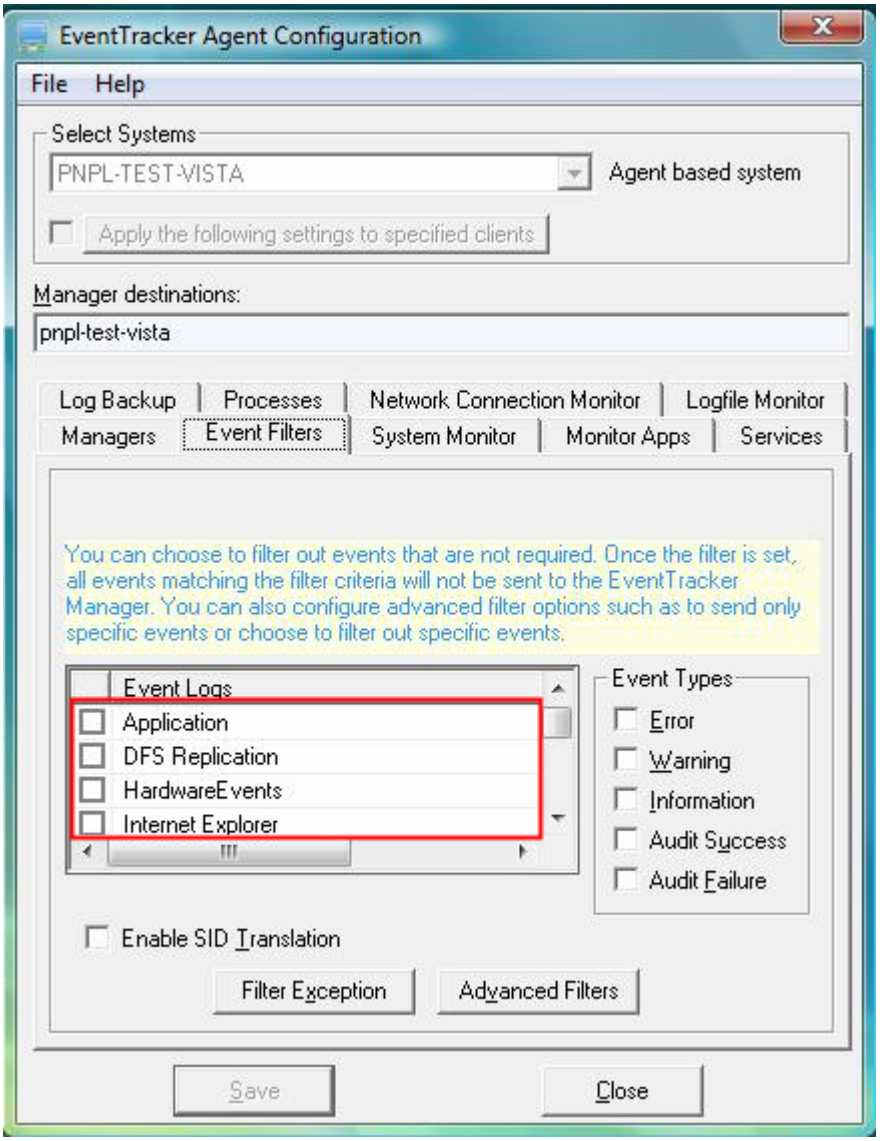
Installing / Uninstalling Vista Agent

Installation and uninstallation procedure for Vista Agent is identical to the procedures for other Windows Agents. No other additional configuration settings are required.

Filtering Events

Event Logs is a dynamic list of Channels. Whenever a new Channel is provided for subscription, EventTracker updates this list automatically. High performance mode is not available for Vista Agent.

Figure 213 Vista Agent Configuration window – Event Filters tab



Monitoring EVTX Logfiles

This option enables you to monitor Vista event log back up files.

To monitor EVTX log files

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Logfile Monitor** tab.

EventTracker displays the Logfile Monitor tab.

4. Click **Add File Name**.

   EventTracker displays the Enter File Name dialog box.

5. Select the logfile type as **EVTX** from the **Select Logfile Type** drop-down list.

6. Type the path in the **Enter File Name** field (OR) click to locate and select the log file.

   EventTracker displays the Select Folder/File Name dialog box.

7. Go to the appropriate folder and then select the file.

8. Click **OK**.

9. Select the log type from the **EVT Log Type** drop-down list.

10. Click **OK**.

    EventTracker displays the Agent Configuration window with newly added configuration settings.

11. Click **Save**.

Configuring Windows Agent

Accessing the Agent Configuration Window

This section helps you access the **Agent Configuration** window in multiple ways.

To access the Agent Configuration Window through Management console

1. Open the Management Console.
2. Click the **Configure** menu and select the **Configure Agents** option.

To access the Agent Configuration Window through System Manager

1. Click the **Configure** menu and select the **Manage Agents** option in the Management console

   (OR)

   Click **System Manager** on the toolbar.

   EventTracker displays the System Manager.

2. Click the **Options** menu and select the **Configure System** option in the System Manager

   (OR)

Click **Configure Agents** on the toolbar.

To access the Agent Configuration Window through Control Panel

- Double-click **Agent Configuration** on the control panel.

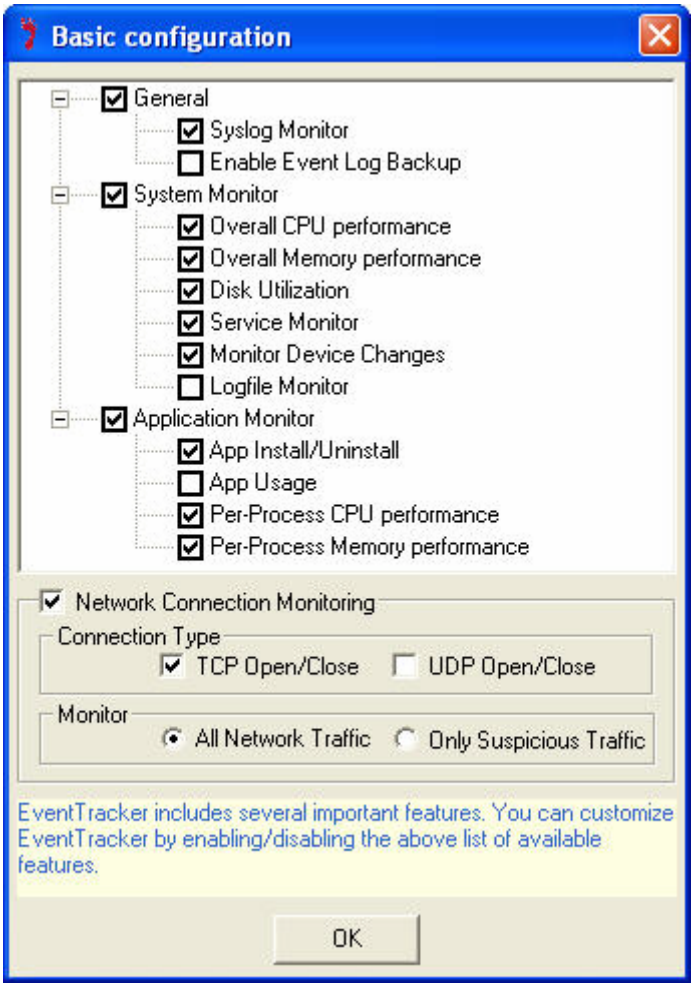
To access the Agent Configuration Window through Programs

- Click **Start**, point to **Programs**, point to **Prism Microsystems**, point to **EventTracker**, and select the **Agent Config** option.

Basic configuration

While installing EventTracker, you have the liberty to set the basic configuration settings.

Figure 214 Basic configuration settings



- Select appropriately and then click **OK**. You can also configure the monitoring options through the Agent Configuration window after installing EventTracker.

Forwarding Events to Multiple Destinations

This option enables you to configure Windows Agent to simultaneously report log events to more than one manager.

To configure Windows Agent to forward Events to multiple managers

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list. EventTracker displays the following messages, if the client is not running on the selected system, or may have older version or the client could not be contacted.

Figure 215 Agent Configuration error message

EventTracker Agent Configuration
Failed to read configuration.
This may be due to :
* Client is not running on the system.
or
* System may have older version of client.
OK

Figure 216 Agent Configuration error message

EventTracker Agent Configuration
Client service could not be contacted on the system.
This system configuration will not be available.
OK

3 Click the **Managers** tab.

4 Click **Add** on the **Managers** tab.

EventTracker displays the Add Destination dialog box.

Figure 217 Add Destination window

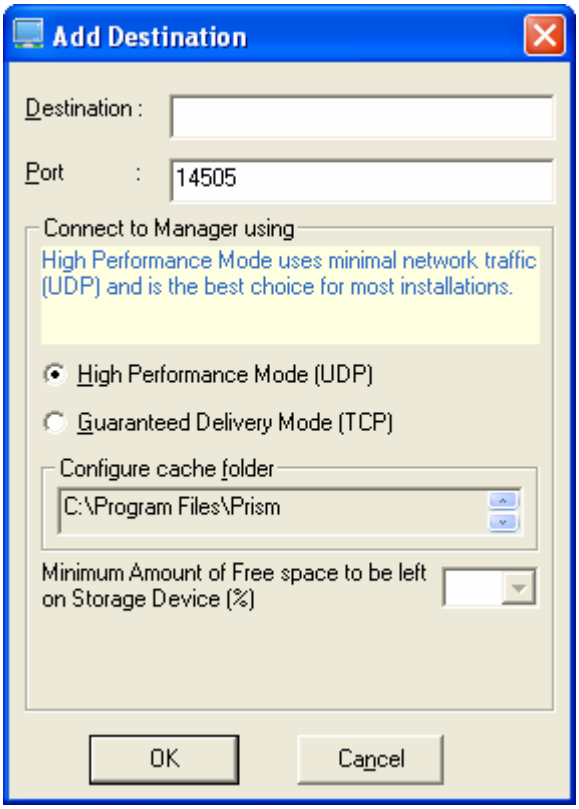

Add Destination
Destination :
Port :
14505
Connect to Manager using
High Performance Mode uses minimal network traffic (UDP) and is the best choice for most installations.
High Performance Mode (UDP)
Guaranteed Delivery Mode (TCP)
Configure cache folder
C:\Program Files\Prism
Minimum Amount of Free space to be left on Storage Device (%)
OK
Cancel

Table 39

Field	Description
Destination	Type the system name in this field. Make sure that EventTracker Manager is installed in the system.
Port	Type the port number in this field. By default, the port number is 14505.
Connect to Manager using	Select the appropriate option. The options are High Performance Mode (UDP) and Guaranteed Delivery Mode (TCP).
Configure cache folder	Select the cache folder. This is used to store events locally on the Agent system when the connection to EventTracker Manager is lost.
Minimum Amount of Free space to be left on Storage Device(%)	This is the feature applies to TCP mode of agent. Actual usage of TCP mode is to deliver the event in a guaranteed way irrespective of connection problems, Receiver status etc. In case if the Agent is not able to communicate with the Receiver, Agent will start storing all the events as cache files in the specified folder (refer: Configure cache folder). If the Receiver is dead for weeks together, Agent keeps storing these files in disk and there by affecting DISK SPACE on critical

Field	Description
	systems. To control this problem, the option "Minimum Amount of Free space to be left on Storage Device(%)" is provided to stop storing events when the disk space is less than the configured number of %. Example, when you configure 20%, Agent will stop writing events to disk when the free space goes down beyond 20%. All these apply only to TCP mode.

5. Type the name of the manager in the **Destination** field.
6. Click **OK**.

   EventTracker displays the Agent Configuration window with the newly added manager.
7. Click **Save**.

   You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Event Delivery modes

EventTracker Agents send the event logs garnered to the Manager, either in High Performance mode (UDP) or in Guaranteed Delivery Mode (TCP).

Since UDP is a connectionless network service, there is no guarantee that the Manager will receive all the data blocks transported by the UDP.

In TCP mode, is a connection oriented network service, there is a guarantee that the Manager will receive all the data packets transported by the TCP.

Modifying Event delivery modes

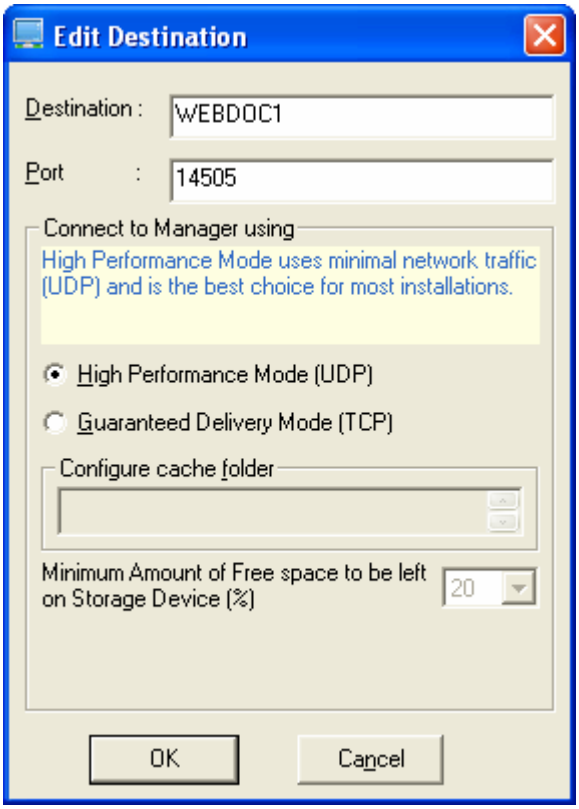
This option helps you modify event delivery modes.

To modify Event delivery mode

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Select the Manager Name from the list in the **Managers** tab.
4. Click **Edit** on the **Managers** tab.

   EventTracker displays the Edit Destination dialog box.

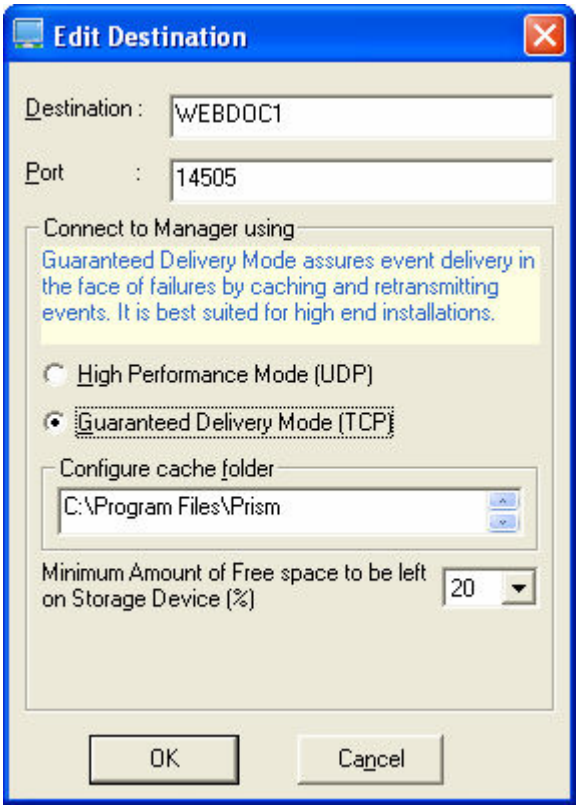
Figure 218 Edit Destination window



By default, EventTracker selects the High Performance Mode (UDP) option.

5 Select the **Guaranteed Delivery Mode (TCP)** option.

Figure 219 Edit Destination window


Edit Destination
Destination :
WEBDOC1
Port :
14505
Connect to Manager using
Guaranteed Delivery Mode assures event delivery in the face of failures by caching and retransmitting events. It is best suited for high end installations.
High Performance Mode (UDP)
Guaranteed Delivery Mode (TCP)
Configure cache folder
C:\Program Files\Prism
Minimum Amount of Free space to be left on Storage Device (%)
20
OK
Cancel

By default, EventTracker stores the cache in the C:\Program Files\Prism Microsystems\EventTracker\Agent\ged folder. You can also modify, if you prefer a different folder to store cache.

6. Type the path of the cache folder in the **Configure cache folder** field.
7. Set **Minimum Amount of Free space to be left on Storage Device (%)**.
8. Click **OK**.
9. Click **Save** on the Agent Configuration window.

   You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 286.

Removing Managers

This option helps you remove Managers.

To remove Managers

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.

3 Select the Manager Name from the list in the **Managers** tab.

4 Click **Remove**.

5 Click **Save** on the Agent Configuration window.

Filtering Events

This option enables you to filter events being sent to the Manager. Select appropriate check boxes under Basic Logs, Special Logs and Event Types.

To filter events

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Event Filters** tab.

EventTracker displays the Event Filters tab.

Figure 220 Agent Configuration window – Event Filters tab

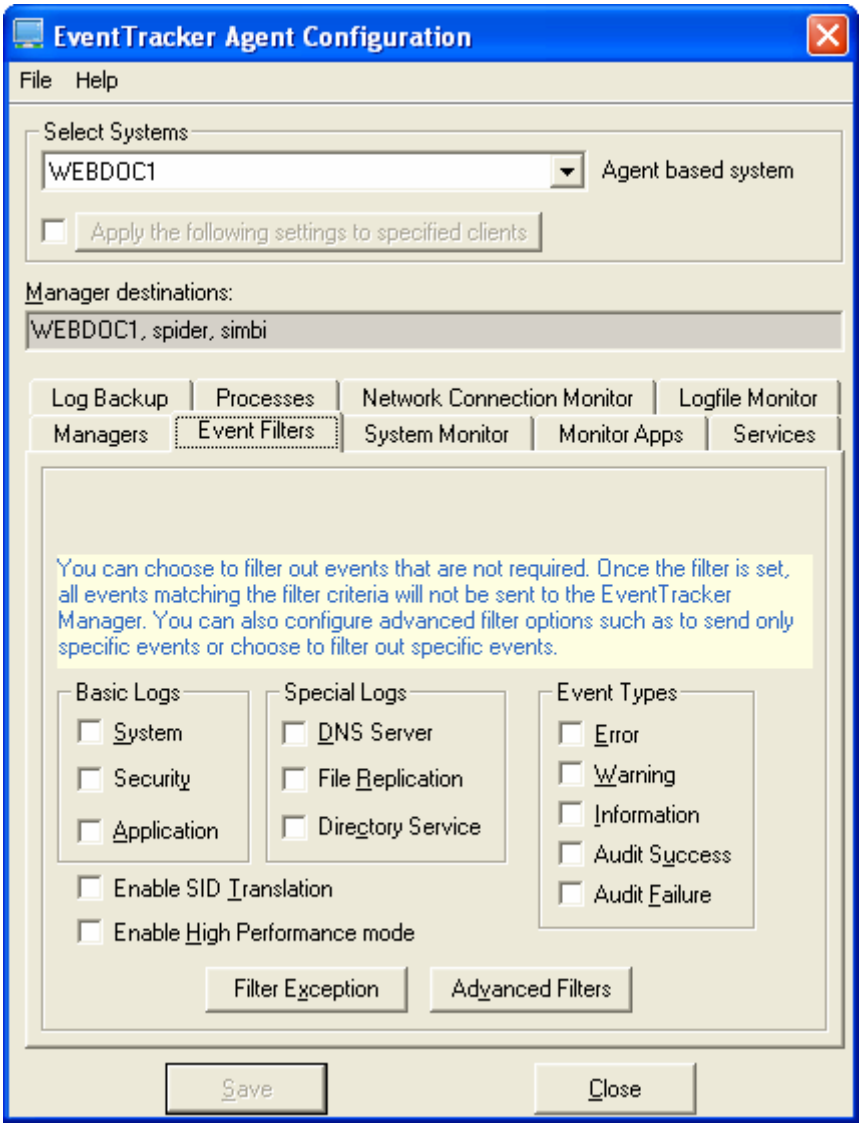


Table 40

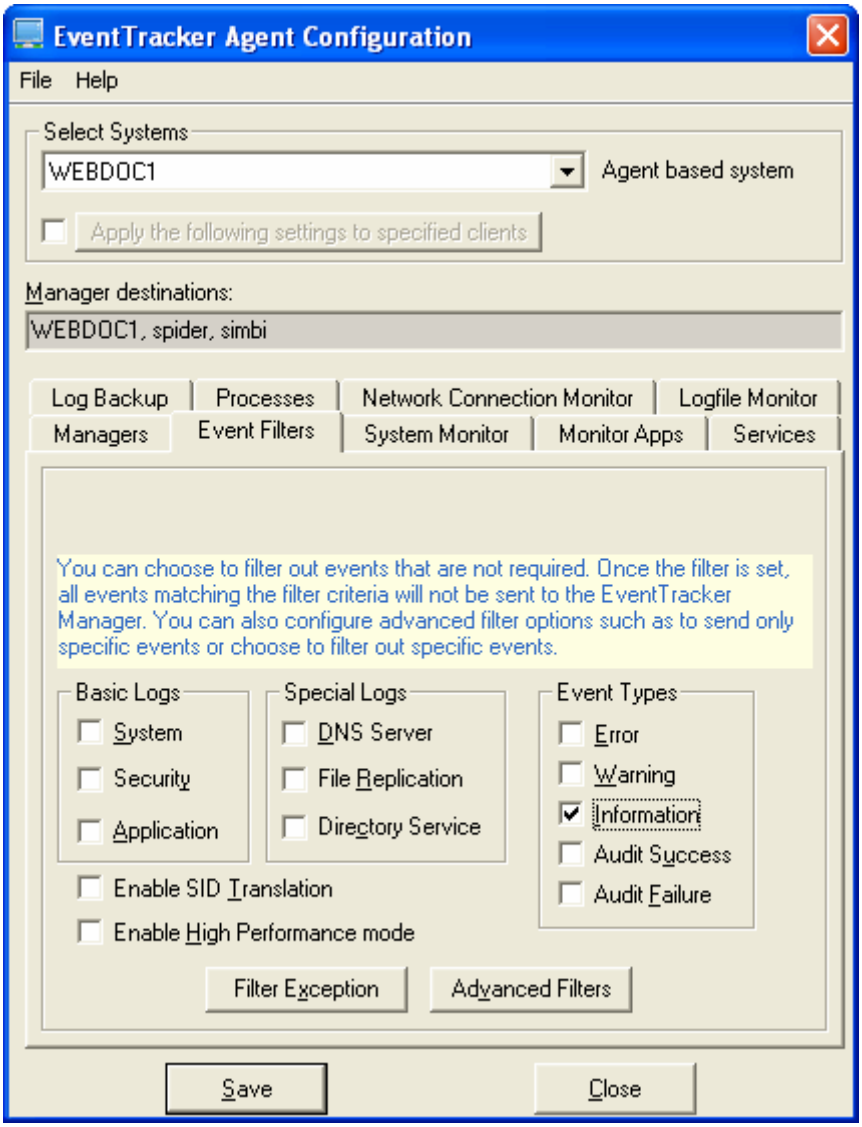
Field	Description
Select Systems	Select a system from the drop-down list for which you want to filter events.
Basic Logs	Select appropriate check boxes to filter the events being sent to the Manager.
Special Logs	Select appropriate check boxes to filter the events being sent to the Manager.
Event Types	Select appropriate check boxes to filter the events being sent to the Manager.
Enable SID	Select this check box for SID translation. For more information

Field	Description
Translation	on SID translation, refer SID-translate.pdf in the EventTracker installation folder.
Enable High Performance mode	Select this check box to switch the Agent modes.
Filter Exception	Click this button to set the filter exceptions for the specific events that you want to monitor.
Advanced Filters	Click this button to set the filters for the specific events that you do not want to monitor.

4 Select appropriately in the relevant fields.

EventTracker displays the Event Filters tab with the newly added filter.

Figure 221 Agent Configuration window – Event Filters tab



Note

The filters are now set and all events with log type event type **Information** will be filtered out and will not be sent to EventTracker Manager.

5 Click **Save**.

You can apply the current settings to other specified Agents. For more information, refer to Applying Configuration Settings to Specified Agents on page 285.

Filtering Events with Exception

This option helps you filter events with exception.

To filter events with exceptions

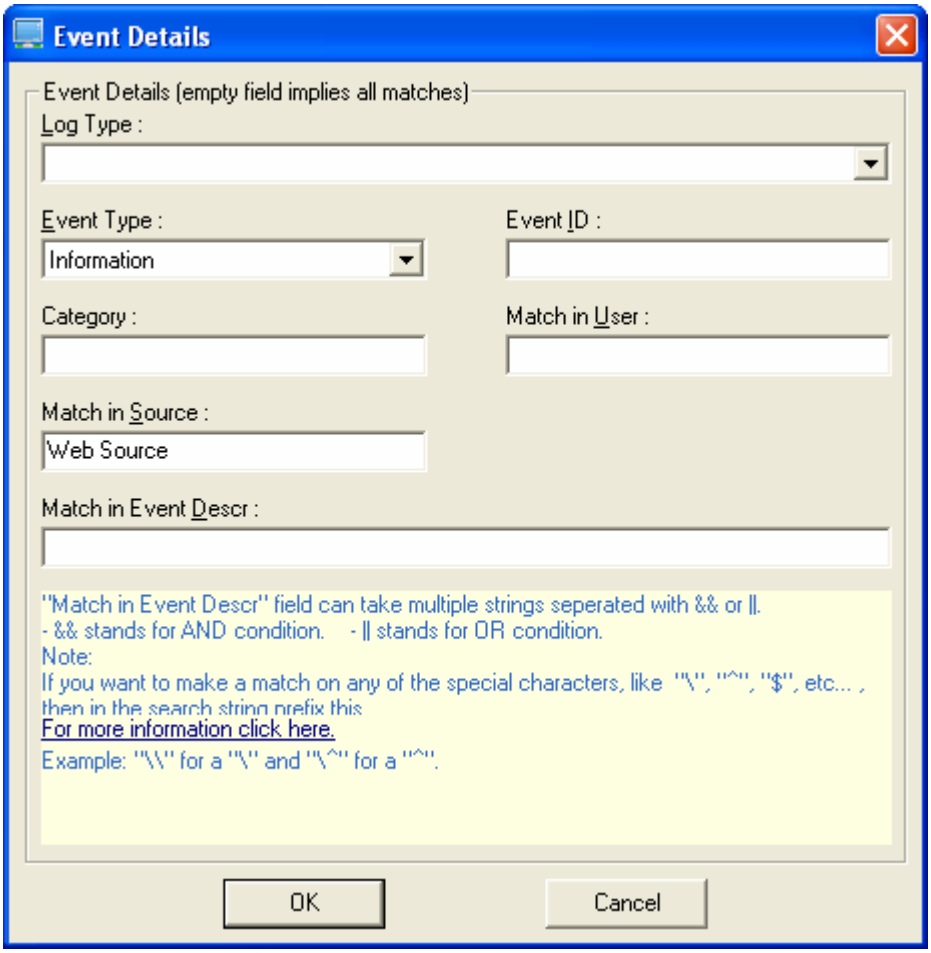
1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Event Filters** tab.
4. Select the check boxes near the event types to filter out the events.

   EventTracker displays the Event Filters tab.
5. Click **Filter Exception**.

   EventTracker displays the Filter Exception dialog box.
6. Click **New**.

   EventTracker displays the Event Details dialog box.
7. Type appropriately in the relevant fields.

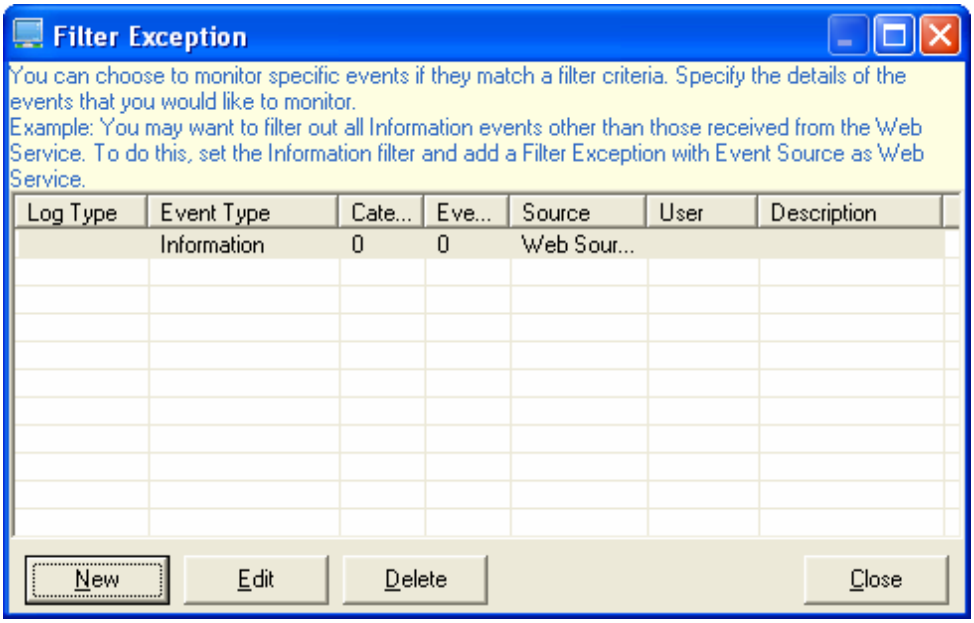
Figure 222 Event Details window


Event Details
Event Details (empty field implies all matches)
Log Type :
Event Type :
Information
Event ID :
Category :
Match in User :
Match in Source :
Web Source
Match in Event Descr :
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... ,
then in the search string prefix this
For more information click here.
Example: "\\" for a "\" and "\^" for a "^".
OK
Cancel

8 Click **OK**.

EventTracker displays the Filter Exception dialog box with the newly added filter exception.

Figure 223 Filter Exception window


Filter Exception
You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.
Log Type
Event Type
Cate...
Eve...
Source
User
Description
Information
0
0
Web Sour...
New
Edit
Delete
Close

9 To modify the settings, select the event in the list, and click **Edit**. Modify the details in the **Event Details** dialog box and click **OK**.

10 To delete the settings, select the event in the list, and click **Delete**.

11 Click **Close** on the Filter Exception dialog box.

> **Note**
>
> All information events will be filtered out with one exception Source: `Web Service`.

12 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer to Applying Configuration Settings to Specified Agents on page 285.

Filtering Events with Advanced Filters

Filters and Filter Exception go hand in hand, which means you can filter all the events but with exceptions. Whereas Advanced Filters help you filter out a specific event allowing other events of that type.

To filter events with Advanced Filters

1 Open the Agent Configuration window.

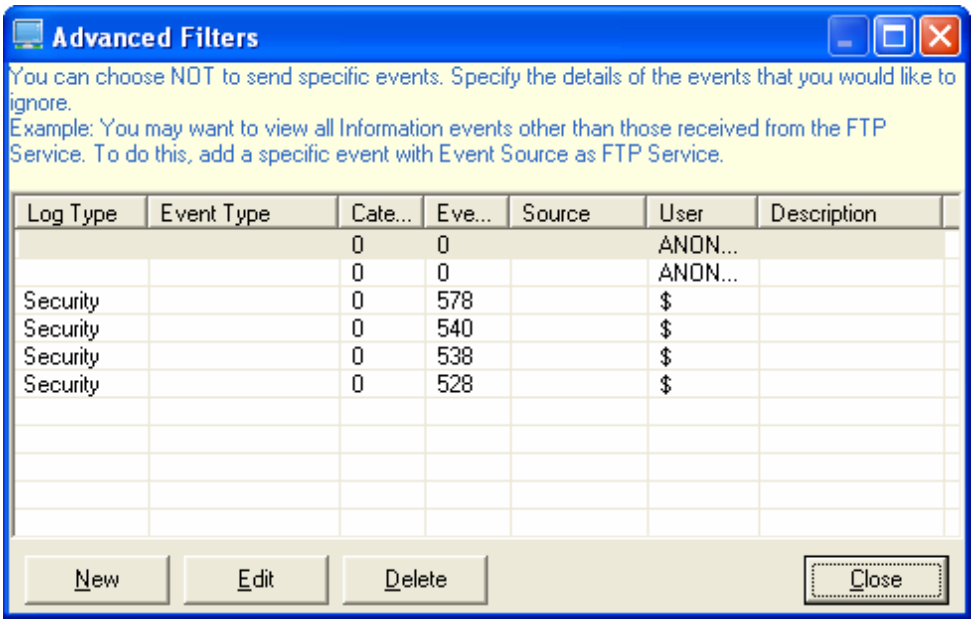
2 Select the system from the **Select Systems** drop-down list.

3 Click the **Event Filters** tab.

4 Click **Advanced Filters**.

EventTracker displays the Advanced Filters dialog box.

Figure 224 Advanced Filters window

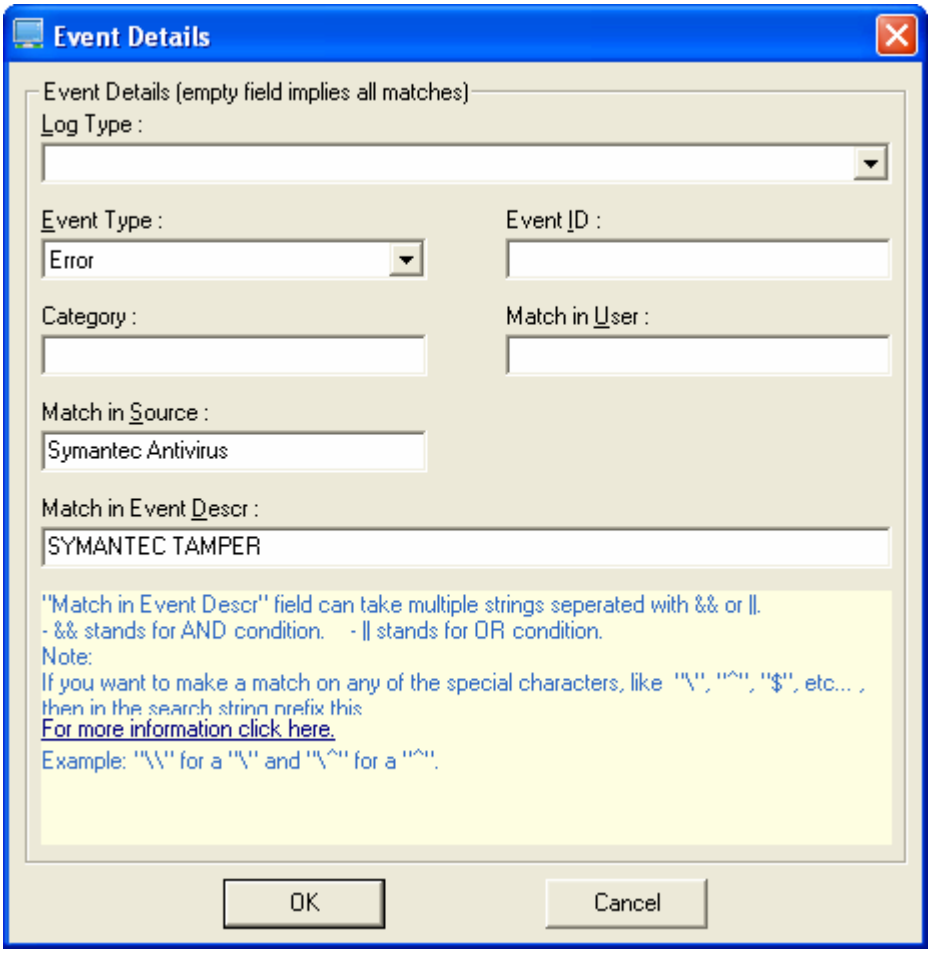

Advanced Filters
You can choose NOT to send specific events. Specify the details of the events that you would like to ignore.
Example: You may want to view all Information events other than those received from the FTP Service. To do this, add a specific event with Event Source as FTP Service.
Log Type
Event Type
Cate...
Eve...
Source
User
Description
0 0 ANON...
0 0 ANON...
Security 0 578 $
Security 0 540 $
Security 0 538 $
Security 0 528 $
New
Edit
Delete
Close

5 Click **New**.

EventTracker displays the Event Details dialog box.

6 Type appropriately in the relevant fields.

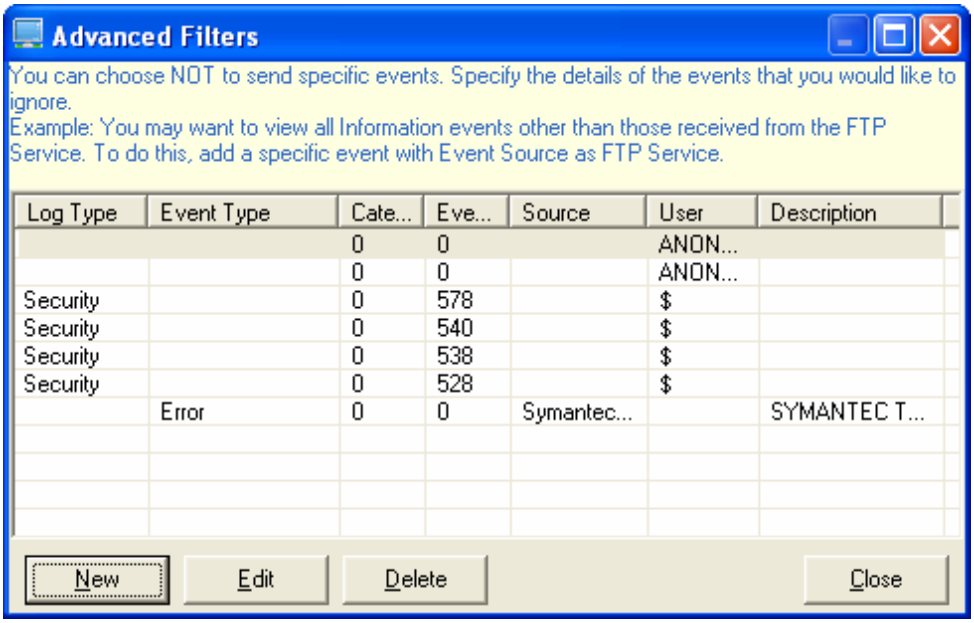
Figure 225 Event Details window


Event Details
Event Details (empty field implies all matches)
Log Type :
Event Type :
Error
Event ID :
Category :
Match in User :
Match in Source :
Symantec Antivirus
Match in Event Descr :
SYMANTEC TAMPER
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like "\", "^", "$", etc... ,
then in the search string prefix this
For more information click here.
Example: "\\" for a "\" and "\^" for a "^".
OK
Cancel

7 Click **OK**.

EventTracker displays the Advanced Filters dialog box with newly added filter.

Figure 226 Advanced Filters window


Advanced Filters
You can choose NOT to send specific events. Specify the details of the events that you would like to ignore.
Example: You may want to view all Information events other than those received from the FTP Service. To do this, add a specific event with Event Source as FTP Service.
Log Type
Event Type
Cate...
Eve...
Source
User
Description
0 0 ANON...
0 0 ANON...
Security 0 578 $
Security 0 540 $
Security 0 538 $
Security 0 528 $
Error 0 0 Symantec... SYMANTEC T...
New
Edit
Delete
Close

8 To modify the settings, select the event in the list, and click **Edit**. Modify the details in the Event Details dialog box and click then **OK**.

9 To delete the settings, select the event in the list, and click **Delete**.

10 Click **Close** on the **Advanced Filters**.

> **Note**
>
> The filter is set and specific events matching the filter criteria will not be forwarded to EventTracker Manager. All Error Events will be forwarded to the Manager except the events matching the filtered criteria set.

11 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Enabling SID Translation

This option helps you enable SID translation.

To enable SID translation

1 Open the Agent Configuration window.

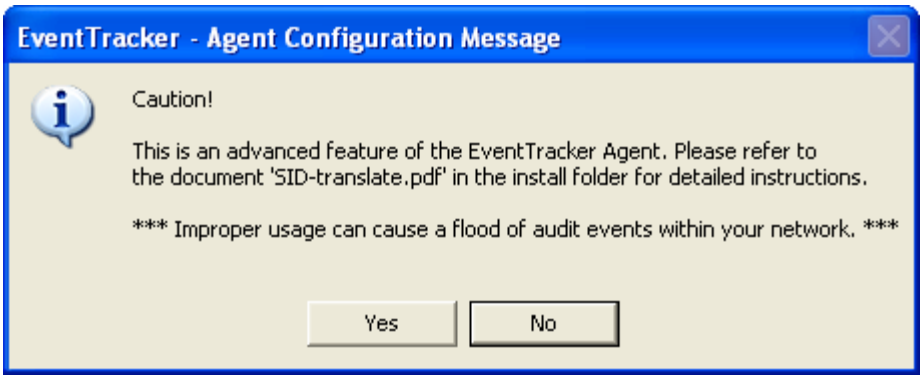
2 Select the system from the **Select Systems** drop-down list.

3 Click the **Event Filters** tab.

4 Select the **Enable SID Translation** check box.

EventTracker displays the EventTracker Agent Configuration message box.

Figure 227
EventTracker Agent Configuration message box


EventTracker - Agent Configuration Message
Caution!
This is an advanced feature of the EventTracker Agent. Please refer to the document 'SID-translate.pdf' in the install folder for detailed instructions.
*** Improper usage can cause a flood of audit events within your network. ***
Yes
No

5 Click **Yes**.

6 Click **Save**.

Note

This feature works in all versions of EventTracker from 5.2 upwards. More information please go through SID-translate.pdf found in the EventTracker installation folder typically, `...\Program Files\Prism Microsystems\EventTracker`.

Enabling High Performance mode

This option helps you enable High Performance mode.

To enable High Performance mode

1 Open the Agent Configuration window.

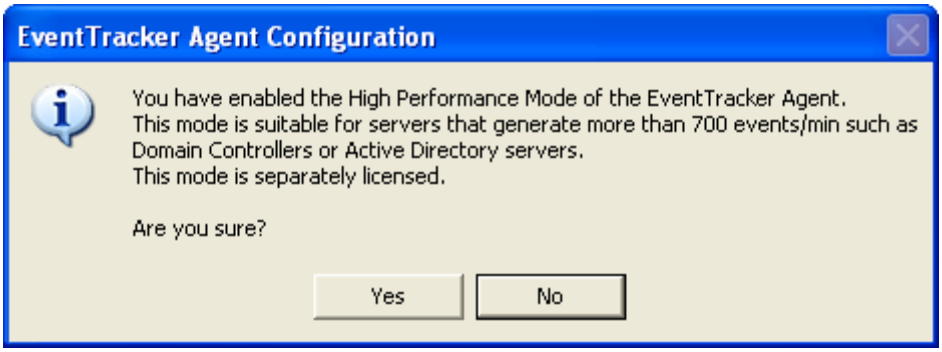
2 Select the system from the **Select Systems** drop-down list.

3 Click the **Event Filters** tab.

4 Select the **Enable High Performance mode** check box.

EventTracker displays the EventTracker Agent Configuration message box.

Figure 228
EventTracker Agent Configuration message box


EventTracker Agent Configuration
You have enabled the High Performance Mode of the EventTracker Agent.
This mode is suitable for servers that generate more than 700 events/min such as Domain Controllers or Active Directory servers.
This mode is separately licensed.
Are you sure?
Yes
No

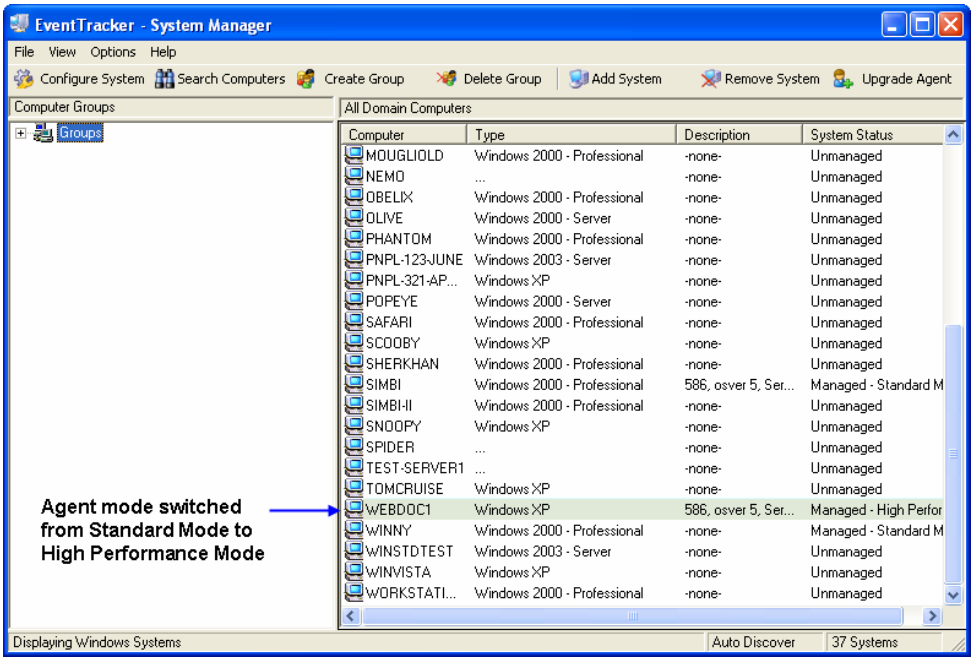
5 Click **Yes**.

6 Click **Save**.

7 Open the System Manager.

EventTracker displays the Agent mode switched to High Performance mode.

Figure 229
EventTracker System Manager


EventTracker - System Manager
File View Options Help
Configure System Search Computers Create Group Delete Group Add System Remove System Upgrade Agent
Computer Groups
Groups
All Domain Computers
Computer Type Description System Status
MOUGLIOLD Windows 2000 - Professional -none- Unmanaged
NEMO ... -none- Unmanaged
OBELIX Windows 2000 - Professional -none- Unmanaged
OLIVE Windows 2000 - Server -none- Unmanaged
PHANTOM Windows 2000 - Professional -none- Unmanaged
PNPL-123-JUNE Windows 2003 - Server -none- Unmanaged
PNPL-321-AP... Windows XP -none- Unmanaged
POPEYE Windows 2000 - Server -none- Unmanaged
SAFARI Windows 2000 - Professional -none- Unmanaged
SCOOBY Windows XP -none- Unmanaged
SHERKHAN Windows 2000 - Professional -none- Unmanaged
SIMBI Windows 2000 - Professional 586, osver 5, Ser... Managed - Standard M
SIMBI-II Windows 2000 - Professional -none- Unmanaged
SNOOPY Windows XP -none- Unmanaged
SPIDER ... -none- Unmanaged
TEST-SERVER1 ... -none- Unmanaged
TOMCRUISE Windows XP -none- Unmanaged
WEBDOC1 Windows XP 586, osver 5, Ser... Managed - High Perfor
WINNY Windows 2000 - Professional -none- Managed - Standard M
WINSTDTEST Windows 2003 - Server -none- Unmanaged
WINVISTA Windows XP -none- Unmanaged
WORKSTATI... Windows 2000 - Professional -none- Unmanaged
Agent mode switched from Standard Mode to High Performance Mode
Displaying Windows Systems
Auto Discover
37 Systems

Monitoring System Health

Monitoring CPU, memory performance and disk usage of a system enables the administrator to keep tabs on the general health of a system. You can configure general health thresholds for CPU and Memory Usage. All thresholds are measured in percent terms.

When the configured threshold is crossed, an event will be generated and reported to the Manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. So, when an event is seen that a system is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

The default threshold limits are 80% for all variables. A configuration of 0% would disable the monitoring for that specific variable.

USB and other Device Changes option helps to monitor insertion or removal of USB and other media. Also helps to track file transactions that occur in the inserted media.

To configure system performance thresholds

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **System Monitor** tab.

   EventTracker displays the System Monitor tab.

Figure 230 Agent Configuration window – System Monitor tab

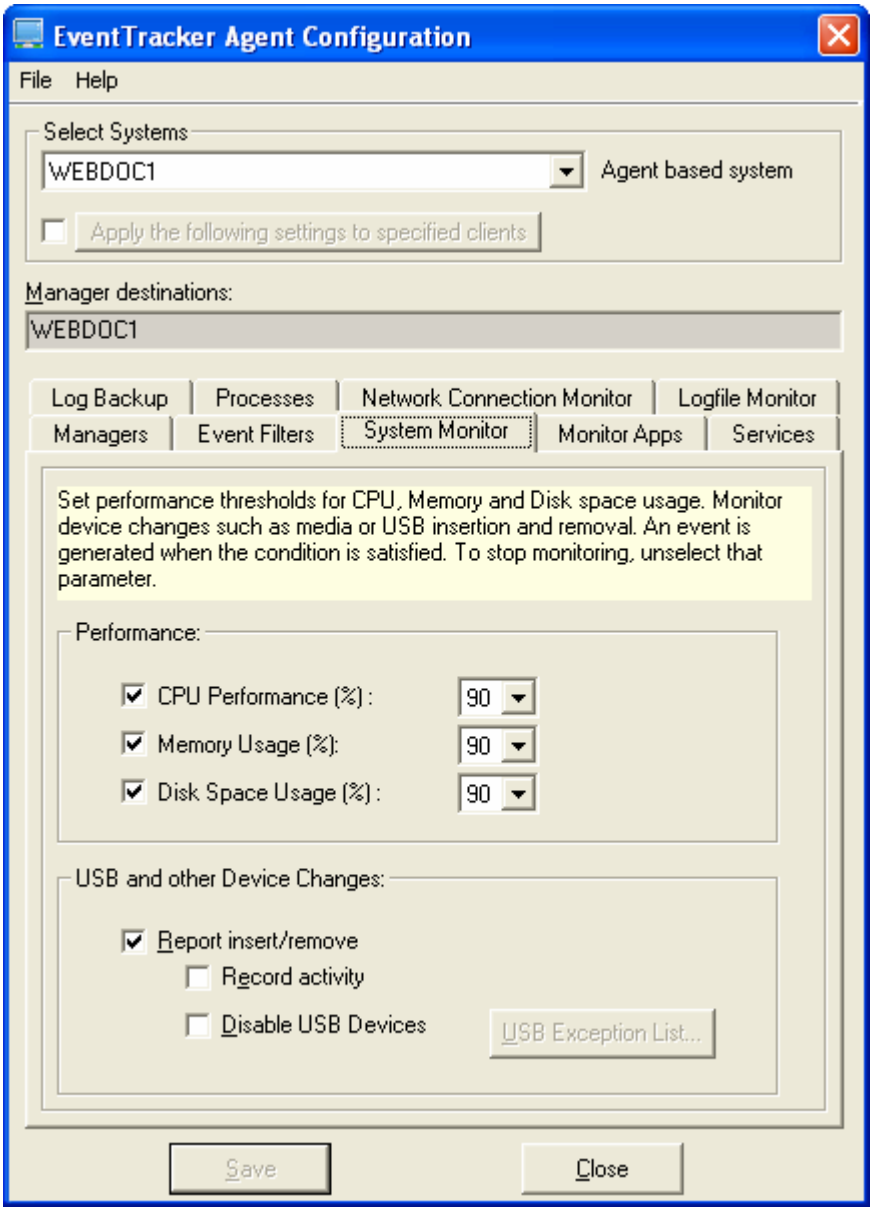
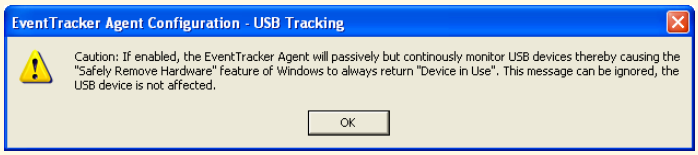


Table 41

Field	Description
Performance	
CPU Performance (%)	Select a threshold limit to monitor CPU performance from the drop-down list.
Memory Usage (%)	Select a threshold limit to monitor memory usage from the drop-down list.

Field	Description
Performance	
Disk Space Usage (%)	Select a threshold limit to monitor disk space usage from the drop-down list.
USB and other Device Changes	
Report insert/remove	Select this check box to track insertion or removal of USB or other devices. This check box is selected by default.
Record activity	Select this check box to monitor file transactions occur in the inserted devices. If you enable this option, EventTracker displays the caution message box.  Click OK to continue.
Disable USB Devices	Select this check box to disable USB devices.
USB Exception List	This button is enabled when you select the Disable USB Devices check box. Click this button to add USB devices that you wish to enable.

4. Set the thresholds appropriately.
5. Set the tracking and monitoring options.
6. Click **Save.**

   You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

USB Exception List

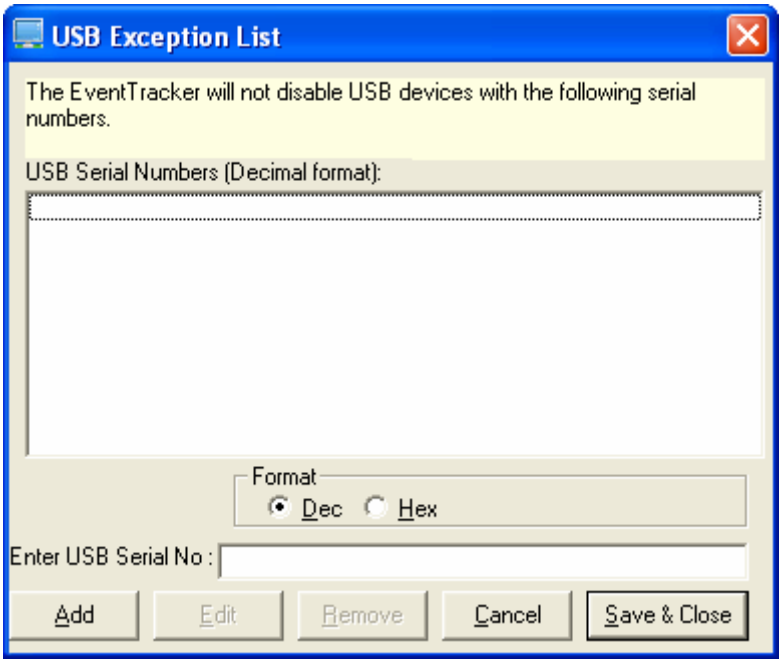
While disabling USB Devices on a particular computer, you can also exempt and enable USB devices from monitoring.

To configure USB exception list

1. Click **USB Exception List**.

   EventTracker displays the USB Exception List dialog box.

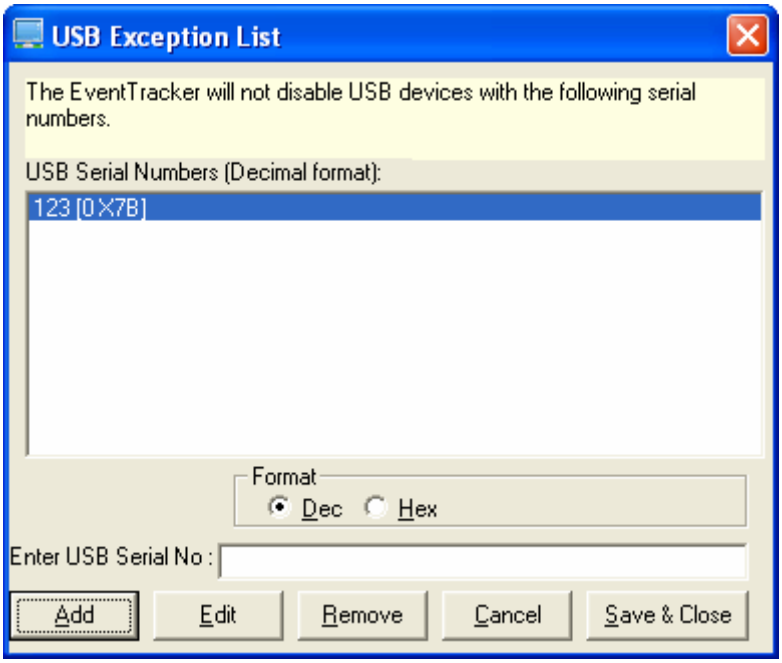
Figure 231 USB Exception List



2. Type the serial no in decimal format in the **Enter USB Serial No** field.
3. To type the serial no in hexadecimal format, select the **Hex** option and then type the serial no in the **Enter USB Serial No** field.
4. Click **Add**.

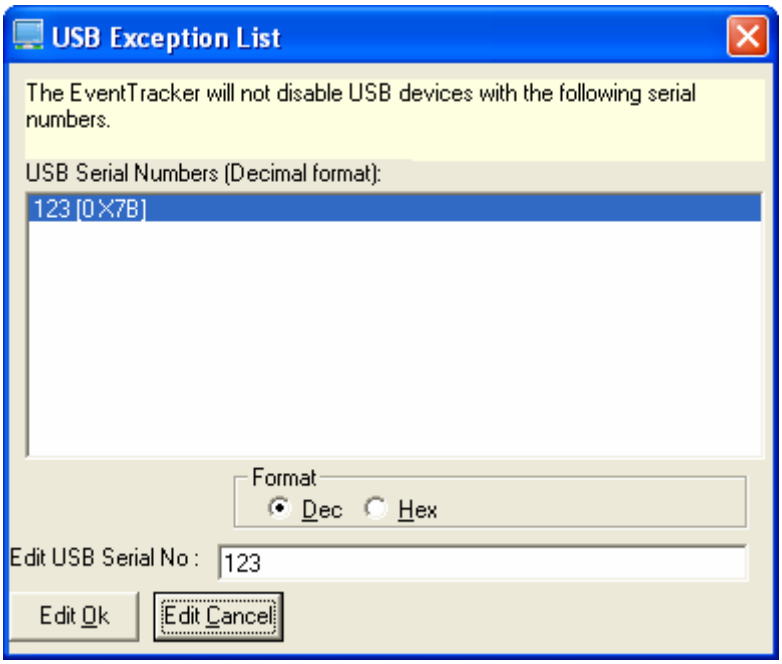
   EventTracker adds the newly entered serial number.

Figure 232 USB Exception List



5 Select a serial number in the list and then click **Edit** to edit the serial number.

Figure 233 USB Exception List



6 Click **Edit Ok** to update the changes or **Edit Cancel** to cancel the changes.

If you click **Edit Ok** without making any changes, EventTracker will displays a message box with appropriate message.

Figure 234 USB Exception List

7 Select a serial number in the list and then click **Remove** to delete the serial number.

8 Click **Cancel** to close the window without saving.

9 Click **Save & Close** to save the changes and close the window.

Monitor Applications

This option enables you to monitor installation and un-installation of applications, and monitor application usage.

EventTracker logs a custom information event whenever a monitored application is opened or closed. These events are received at the Console and helps in tacking the application usage.

EventTracker monitors all applications specified in "Monitor Specific Apps" and ignores applications specified in "App Exception".

The "Monitor Specific Apps" takes precedence over "App Exception". Hence, if an application is specified in both the sections it will be monitored.

To monitor application installation and un-installation

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Monitor Apps** tab.

EventTracker displays the Monitor Apps tab.

Figure 235 Agent Configuration window – Monitor Apps tab

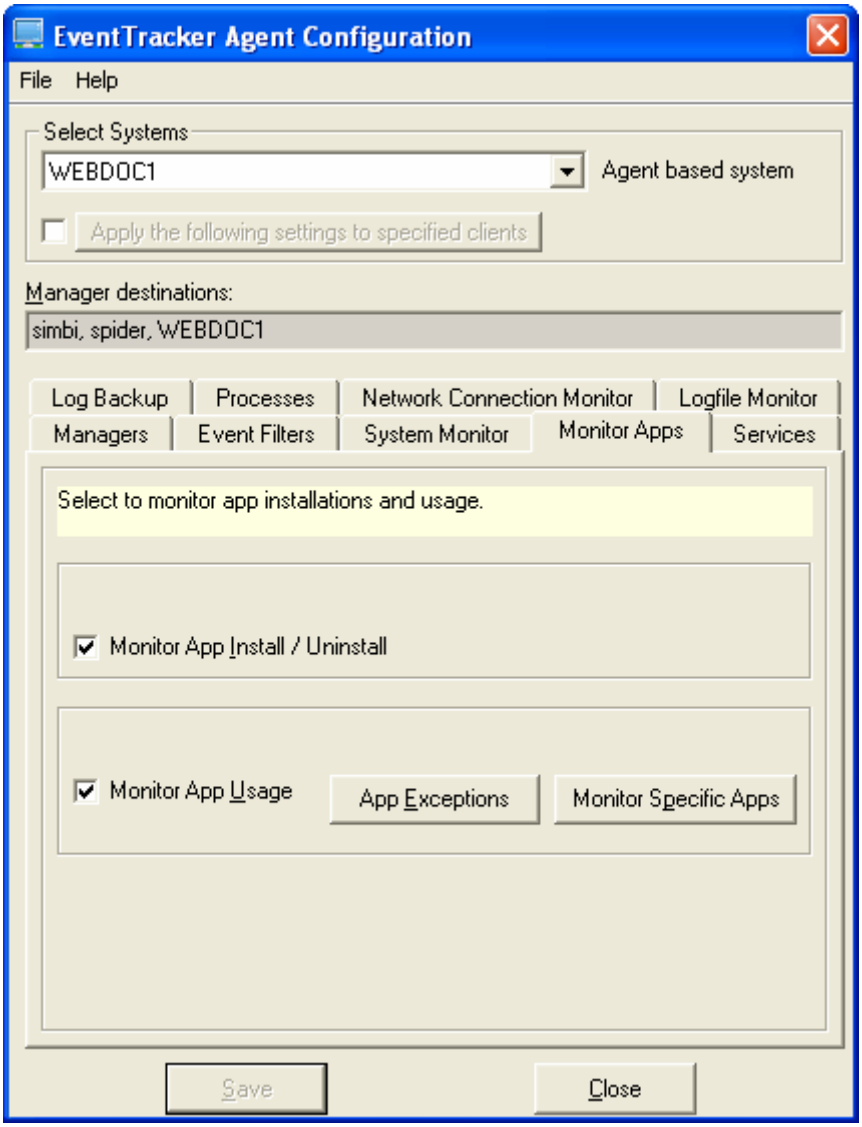


Table 42

Field	Description
Monitor App Install/ Uninstall	Select this check box to monitor installation and un-installation of applications.
Monitor App Usage	Select this check box to monitor application usage. The App Exceptions and Monitor Specific Apps. buttons are enabled. App Exceptions – Enables you to set the applications that you do not want to monitor. Monitor Specific Apps – Enables you to set the applications that you want to monitor.

4 Select appropriately the **Monitor App Install / Uninstall** and **Monitor App Usage** options**.**

5 Click **Save**.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 286.

Filtering applications that need not be monitored

To filter out applications that need not be monitored

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Select the **Monitor App Usage** option.

EventTracker displays the Monitor Apps tab.

4 Click **App Exceptions**.

EventTracker displays the App Exceptions dialog box.

5 Click **Add**.

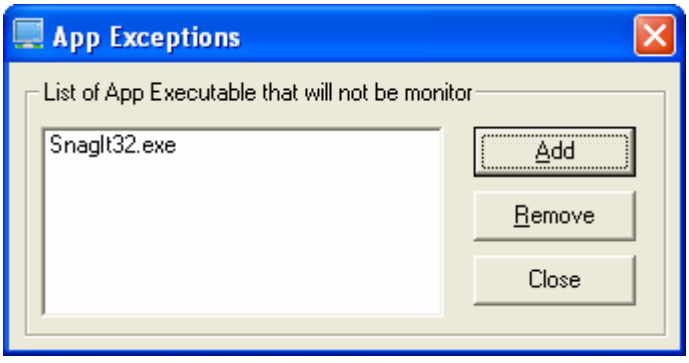
EventTracker displays the EventTracker Agent Configuration dialog box.

6 Type the application name with `.exe` extension that you do not want to monitor.

7 Click **OK**.

EventTracker displays the App Exceptions dialog box.

Figure 236 App Exceptions window



8 To remove, select the application and click **Remove**.

9 Click **Close**.

10 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer to Applying the Settings to Specified Agents on page 285.

Filtering applications that need to be monitored

To filter out specific applications to monitor

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Select the **Monitor App Usage** option.

EventTracker displays the Monitor Apps tab.

4 Click **Monitor Specific Apps**.

EventTracker displays the Monitor Specific Apps dialog box.

5 Click **Add**.

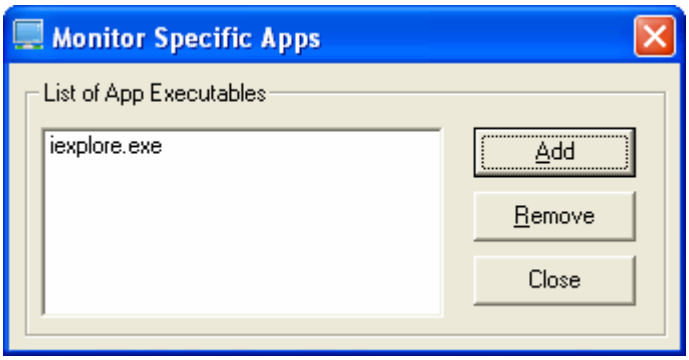
EventTracker displays the EventTracker Agent Configuration dialog box.

6 Type the application name with `.exe` extension that you want to monitor.

7 Click **OK**.

EventTracker displays the Monitor Specific Apps dialog box.

Figure 237 Monitor Specific Apps window



8 To remove, select the application and click **Remove**.

9 Click **Close**.

10 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Monitoring Services

By default, EventTracker monitors all Windows Services for stop/start. If a service stops, an event will be sent immediately to the Manager. An event will also be sent if a stopped service restarts.

You can also choose to automatically restart services that have been stopped.

There may be certain services that you may not want to monitor. You can filter out such services from the monitoring list.

The service name that needs to be configured can be either the name as displayed in Control Panel -> Services or the display name. While configuring the service name, please ensure that it is spelt correctly.

To configure services that needs to be restarted on stopping

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Services** tab.

   EventTracker displays the Services tab.

Figure 238 Agent Configuration window – Services tab

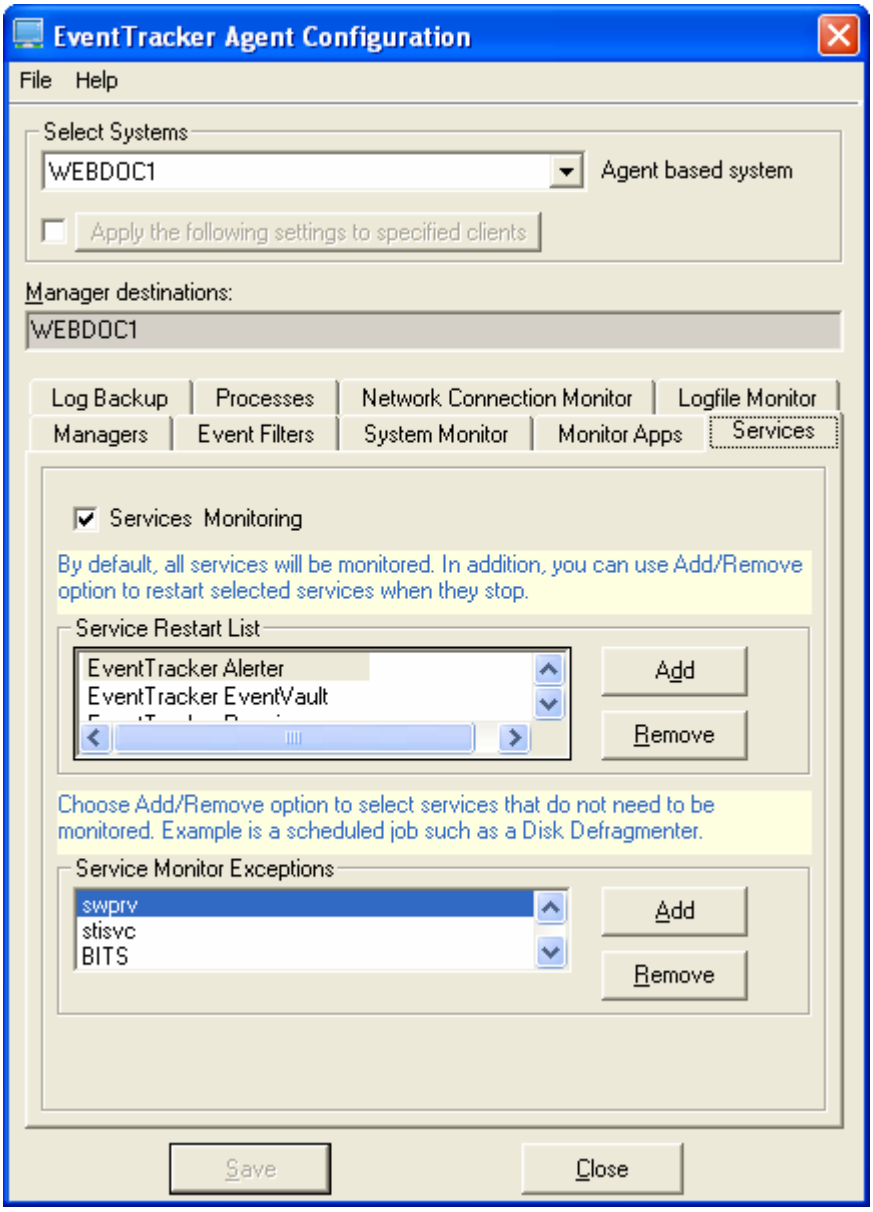


Table 43

Field	Description
Services Monitoring	This check box is selected by default to monitor all Windows services. **Add** and **Remove** buttons of Service Restart List and Service Monitor Exceptions are disabled if you clear this check box.
Service Restart List	By default, EventTracker Alerter, EventTracker Scheduler, EventTracker Receiver, EventTracker EventVault and

Field	Description
	WcwService services are monitored. Click **Add** to add selected services to restart when they stop. Click **Remove** to remove the services from the list.
Service Monitor Exceptions	Click **Add** to add services that you do not want to monitor. Click **Remove** to remove the services from the list.

4 Click **Add** next to **Service Restart List**.

EventTracker displays the EventTracker Agent Configuration dialog box.

5 Type the name of the service in the **Enter Service Name** field.

6 Click **OK**.

EventTracker adds the service to the Service Restart List.

7 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Filtering Services that need not be monitored

To filter out services that need not be monitored

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Services** tab.

EventTracker displays the Services tab.

4 Click **Add** next to **Service Monitor Exceptions**.

EventTracker displays the EventTracker Agent Configuration dialog box.

5 Type the service that you do not want to monitor in the **Enter Service Name** field.

6 Click **OK**.

EventTracker adds the service to the Service Monitor Exceptions list.

7 Click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Monitoring Logfiles

This option enables you to monitor multi-vendor log files with matching keyword entries. EventTracker generates an event if any matching record is found.

To add a log file to monitor

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Logfile Monitor** tab.

   EventTracker displays the Logfile Monitor tab.

Figure 239 Agent Configuration window – Logfile Monitor tab

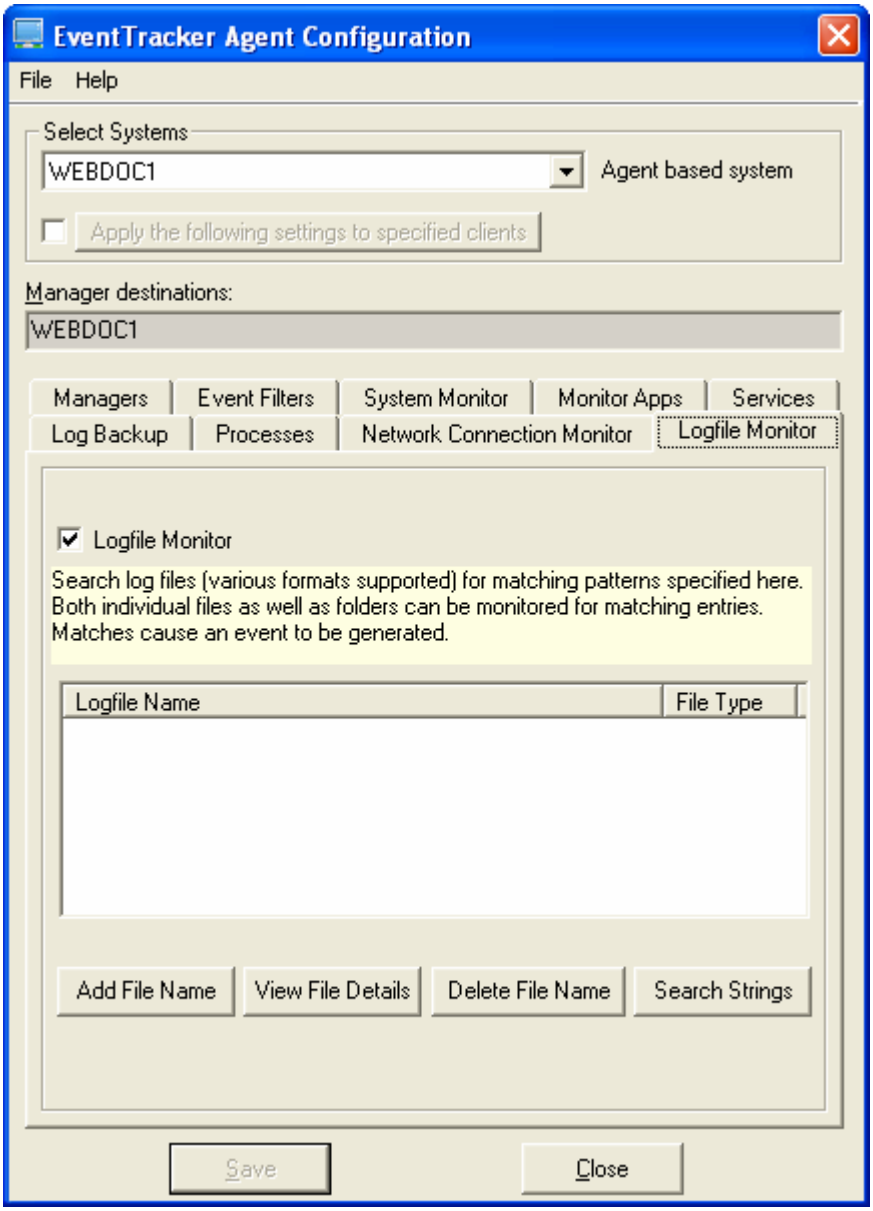


Table 44

Click	To
Add File Name	Add a log file that you want to monitor.
View File Details	View log file details.
Delete File Name	Delete the log file name from the list.
Search Strings	Configure the strings to search.

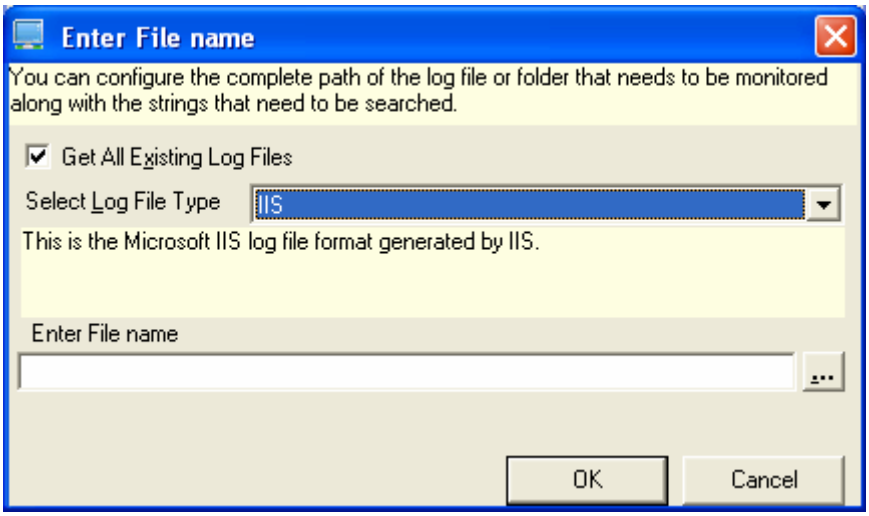
4 Click **Add File Name**.

EventTracker displays the Enter File Name dialog box.

5 Select the **Get All Existing Log Files** option, if you want all the existing files prior to this configuration and the files that are logged after this configuration.

6 Select the logfile type from the **Select Logfile Type** drop-down list.

Figure 240 Enter File Name dialog box


Enter File name
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type
IIS
This is the Microsoft IIS log file format generated by IIS.
Enter File name
OK
Cancel

7 Type the path in the **Enter File Name** field.

(OR)

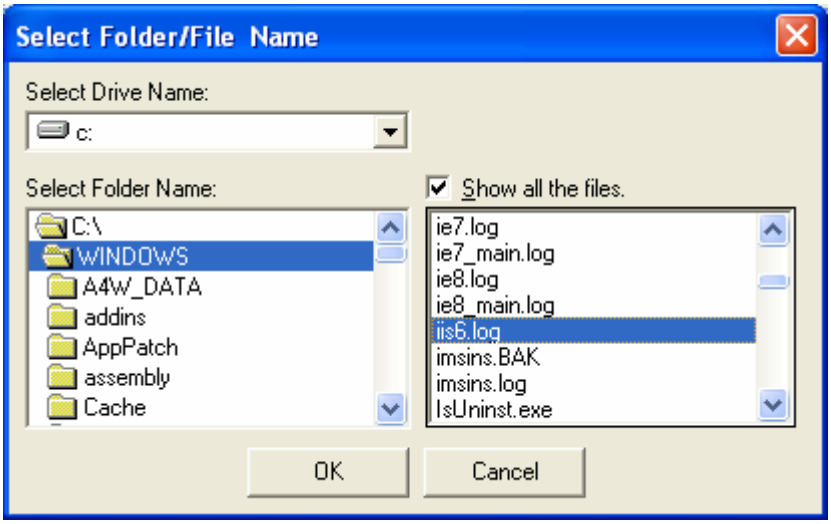
Click to locate and select the log file.

EventTracker displays the Select Folder/File Name dialog box when you click .

8 Go to the appropriate folder, select the **Show all the files** check box to view all files with different file extensions.

9 Select an appropriate file that is associated with the Log File Type selected.

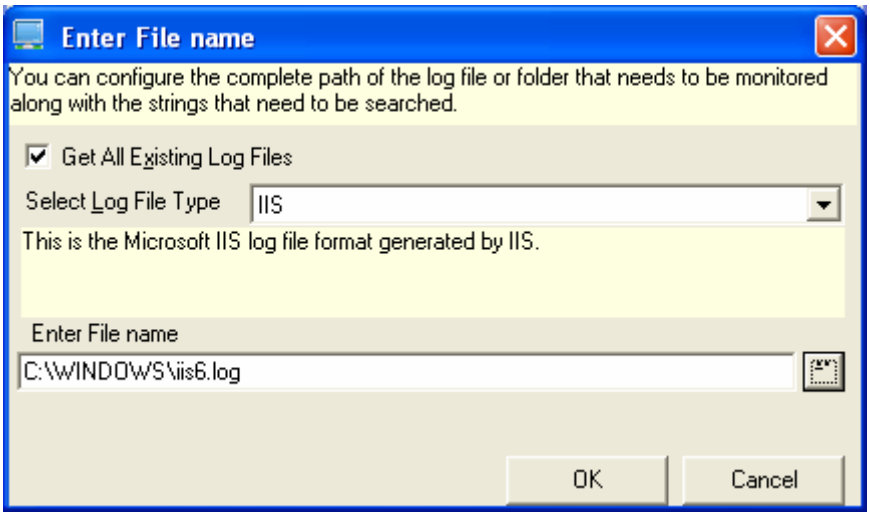
Figure 241 Select Folder/File Name dialog box



10 Click **OK**.

EventTracker displays the Enter File Name dialog box.

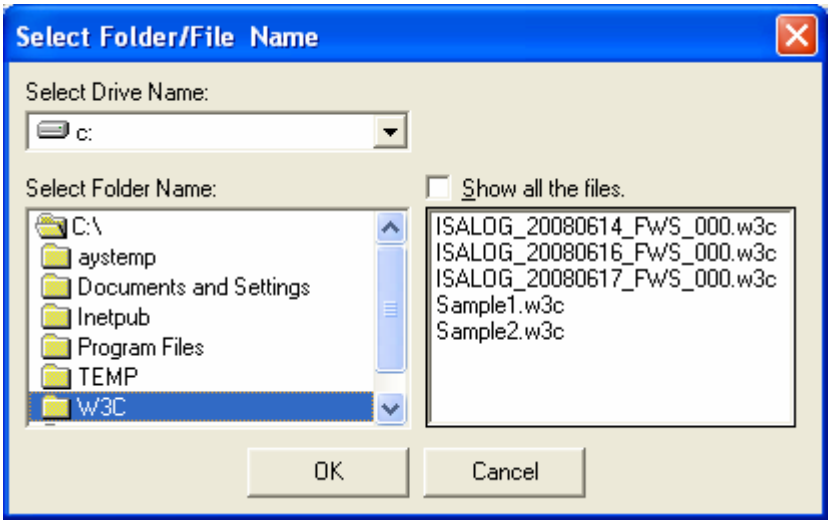
Figure 242 Enter File Name dialog box


Enter File name
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type
IIS
This is the Microsoft IIS log file format generated by IIS.
Enter File name
C:\WINDOWS\iis6.log
OK
Cancel

11 Click **OK**.

You can also select multiple files with the same or different file extension by using wildcard character *****

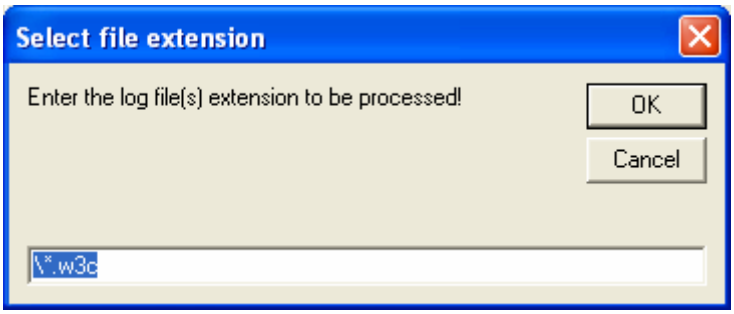
Figure 243 Select Folder/File Name



Click **OK**.

EventTracker displays the Select File Extension window.

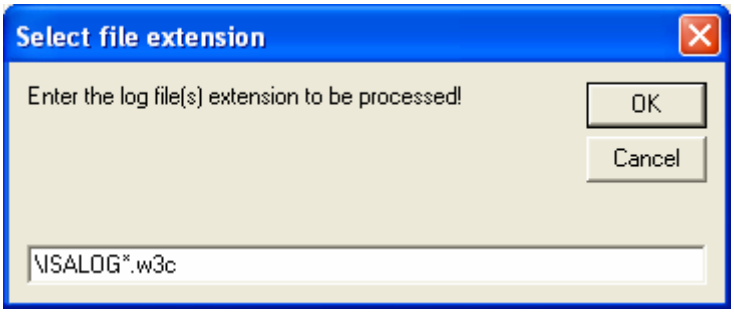
Figure 244 Select file extension



Type the file name in field provided or leave as it is to consider all files in the selected folder with file extension w3c for monitoring.

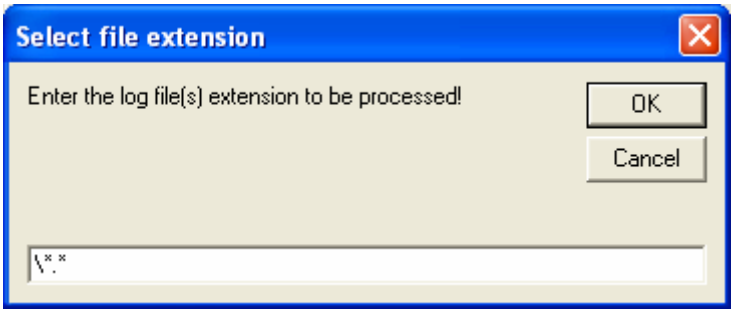
If you are specifically interested in monitoring ISA Firewall log files, type the file name as "ISALOG*"

Figure 245 Select file extension



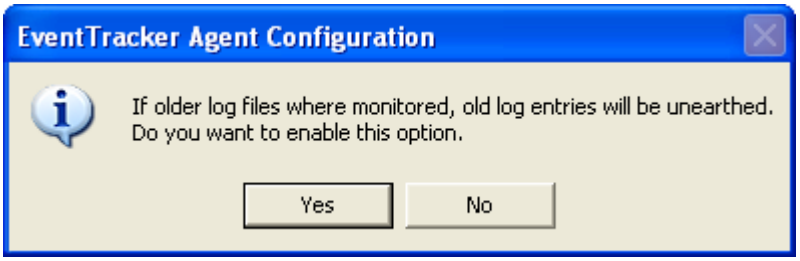
To select multiple files irrespective of file extensions, type *.*

Figure 246 Select file extension



EventTracker displays the EventTracker Agent Configuration message box.

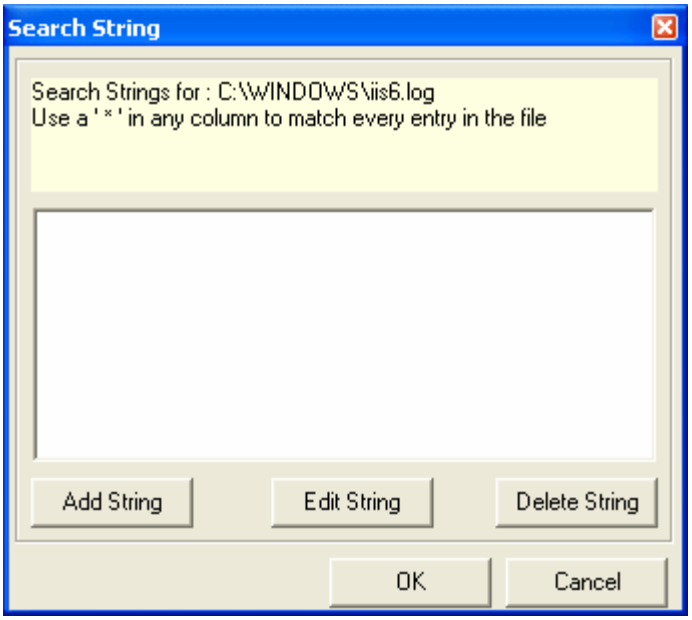
Figure 247 EventTracker Agent Configuration message box


EventTracker Agent Configuration
If older log files where monitored, old log entries will be unearthed.
Do you want to enable this option.
Yes
No

12 Click **Yes**.

EventTracker displays the Search String dialog box.

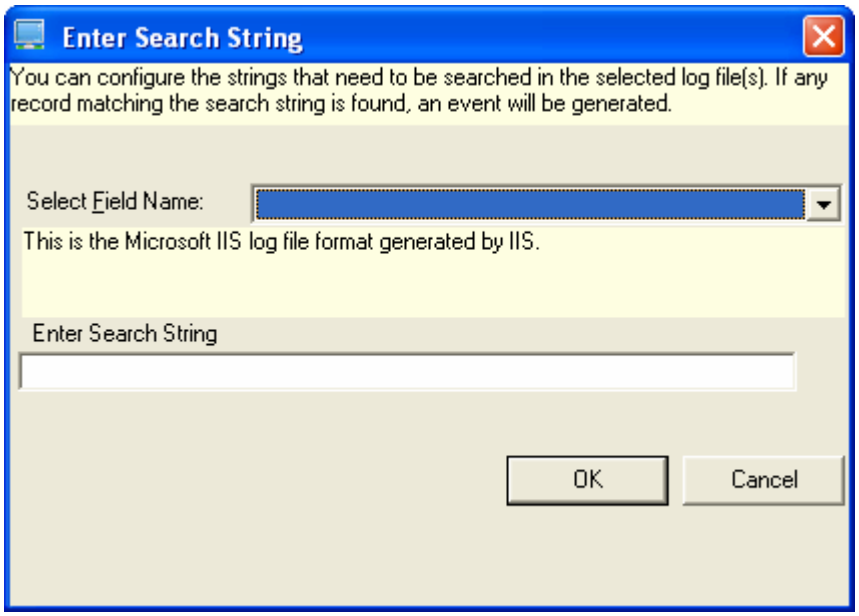
Figure 248 Search String window



13 Click **Add String**.

EventTracker displays the Enter Search String dialog box.

Figure 249 Enter Search String dialog box

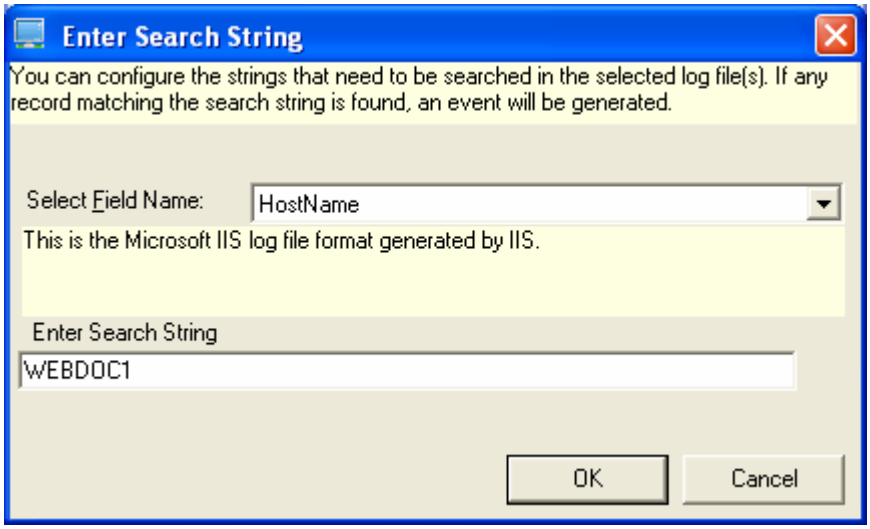

Enter Search String
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.
Select Field Name:
This is the Microsoft IIS log file format generated by IIS.
Enter Search String
OK
Cancel

14 Select the file name from the **Select Field Name** drop-down list.

15 Type the string that you want to search in the **Enter Search String** field.

EventTracker displays the Enter Search String dialog box.

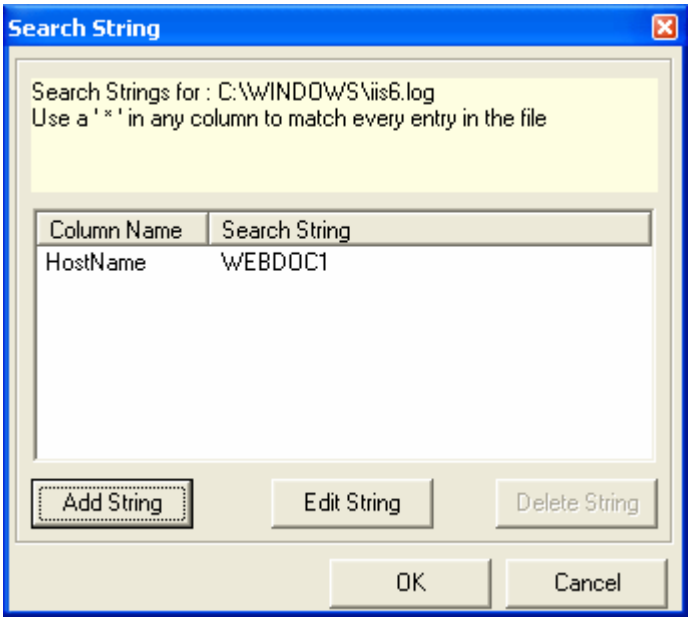
Figure 250 Enter Search String dialog box


Enter Search String
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.
Select Field Name:
HostName
This is the Microsoft IIS log file format generated by IIS.
Enter Search String
WEBDOC1
OK
Cancel

16 Click **OK**.

EventTracker displays the Search String dialog box.

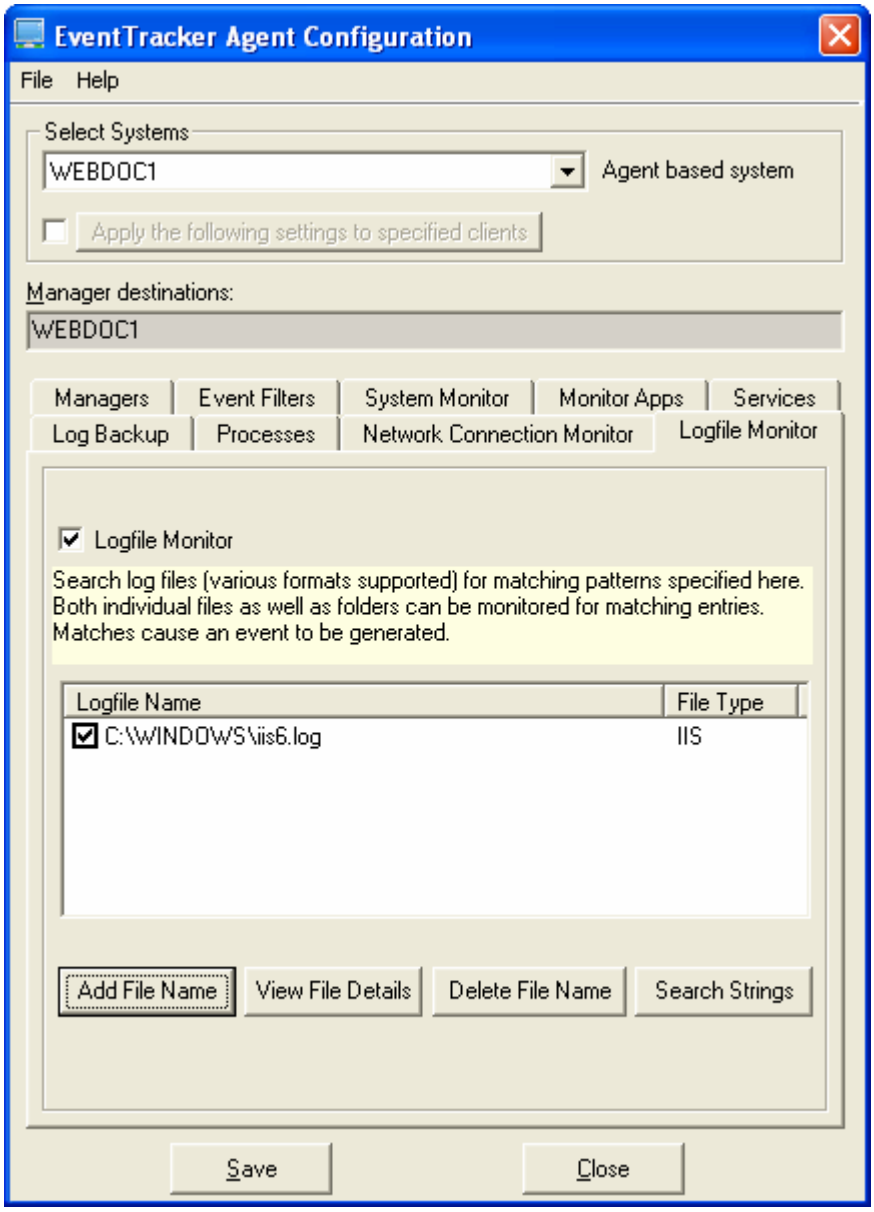
Figure 251 Search String window



17 Click **OK**.

EventTracker displays the Agent Configuration window with the newly added Logfile entry.

Figure 252 Agent Configuration window – Logfile Monitor tab



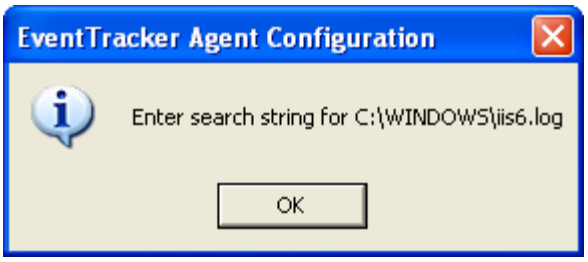
18 Click **Save**.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Clear the check box against the Logfile Name to exclude the file from monitoring.

EventTracker displays the EventTracker Agent Configuration message box, if you try to save without entering the search string for the monitored log file.

Figure 253 EventTracker Agent Configuration message box



Viewing File Details

This option helps you view files details.

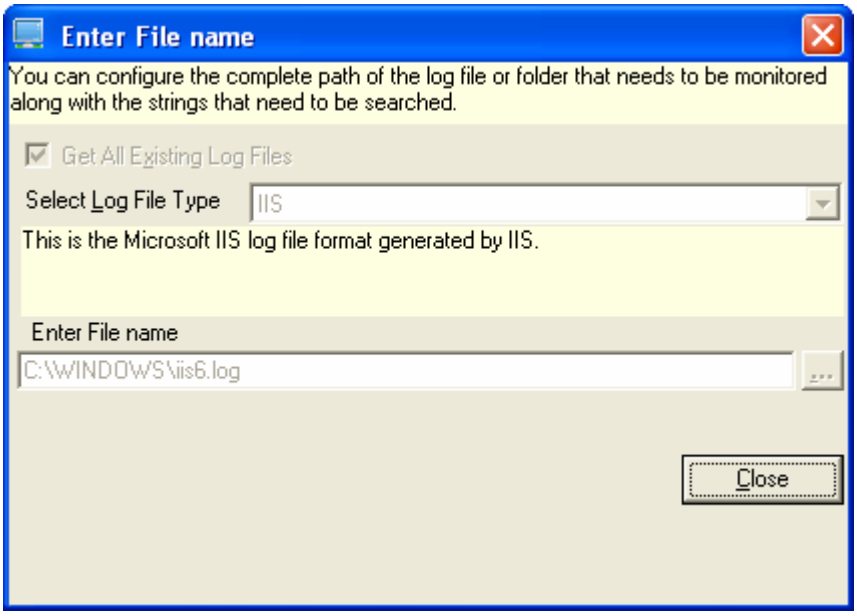
To File Details

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Logfile Monitor** tab.

   EventTracker displays the Logfile Monitor tab.
4. Select the log file from the list under **Logfile Name**.
5. Click **View File Details**.

   EventTracker displays the Enter File Name dialog box.

Figure 254 Enter File Name dialog box


Enter File name
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type
IIS
This is the Microsoft IIS log file format generated by IIS.
Enter File name
C:\WINDOWS\iis6.log
...
Close

6. Click **Close**.

Deleting Log file monitoring settings

This option helps you delete log file monitoring settings.

To delete log file monitoring settings

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Logfile Monitor** tab.
4. Select the log file from the **Logfile Name** list.
5. Click **Delete File Name**.
6. Click **Save** on the Agent Configuration window.

Searching Strings

This option helps you search strings.

To search string

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Logfile Monitor** tab.
4. Select the log file from the **Logfile Name** list.
5. Click **Search Strings**.

Figure 255 Search String window

6 Click **Add String**.

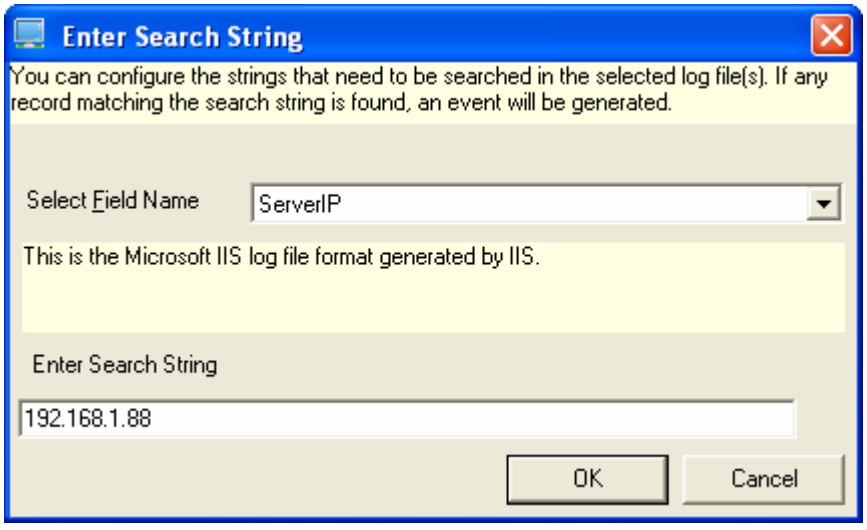
EventTracker displays the Enter Search String dialog box.

7 Select the file name from the **Select Field Name** drop-down list.

8 Type the string that you want to search in the **Enter Search String** field.

EventTracker displays the Enter Search String dialog box with newly added search string entry.

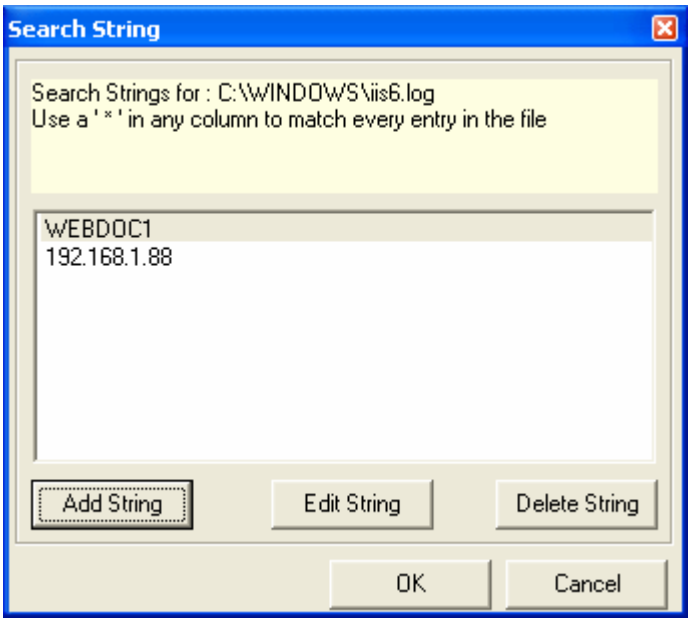
Figure 256 Enter Search String dialog box


Enter Search String
You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.
Select Field Name
ServerIP
This is the Microsoft IIS log file format generated by IIS.
Enter Search String
192.168.1.88
OK
Cancel

9 Click **OK**.

EventTracker displays the Search String dialog box with newly added search string.

Figure 257 Search String window



10 Click **OK**.

EventTracker displays the Agent Configuration window with the modified settings.

11 Click **Save**.

EventTracker displays the EventTracker Agent Configuration message box, if you search strings without any log file entry.

Figure 258 EventTracker Agent Configuration message box

Monitoring Check Point Logs

This option helps you monitor logs generated by Check Point.

To monitor Check Point logs

1 Open the Agent Configuration window.

2 Select the system from the **Select System** drop-down list.

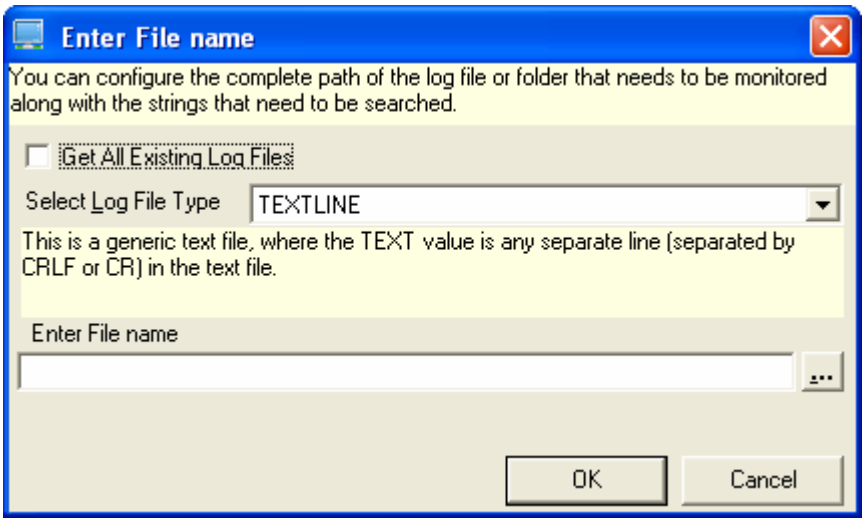
3 Click the **Logfile Monitor** tab.

EventTracker displays the Logfile Monitor tab.

4 Click **Add File Name**.

EventTracker displays the Enter File Name dialog box.

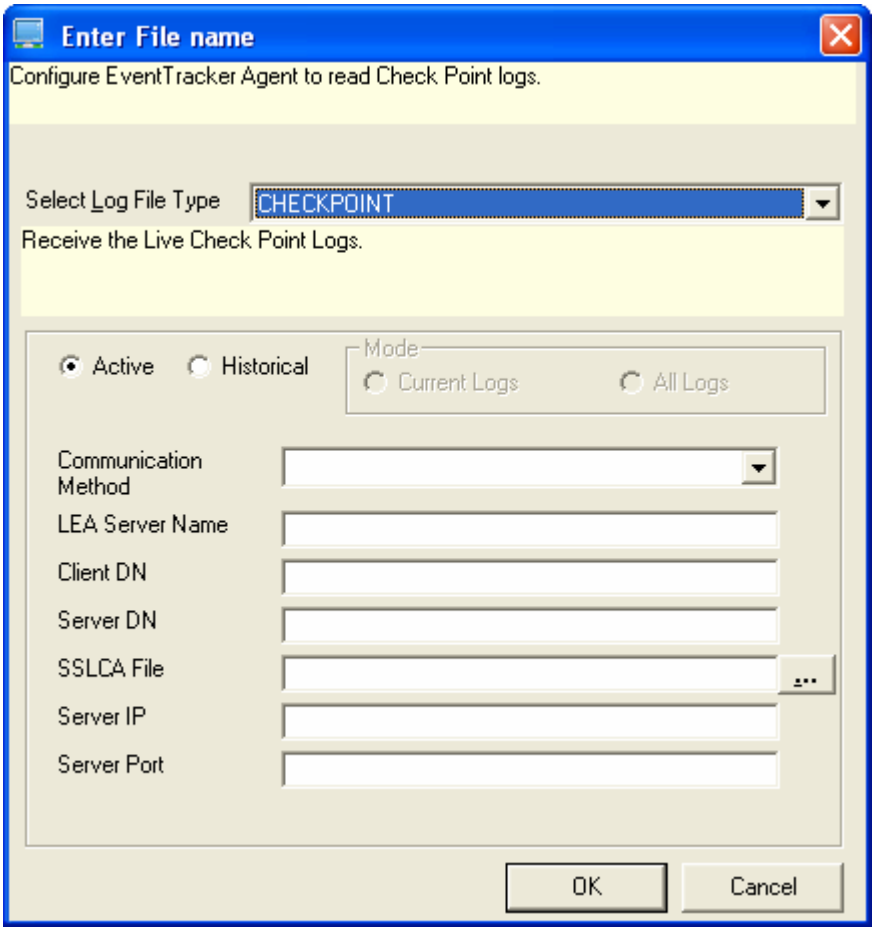
Figure 259 Enter File name dialog box


Enter File name
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type
TEXTLINE
This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.
Enter File name
...
OK
Cancel

5 Select the logfile type as CHECKPOINT from the **Select Logfile Type** drop-down list.

EventTracker displays the Enter File Name dialog box.

Figure 260 Enter File Name dialog box



6 Select and option from the Communication Method drop-down list.

Table 45

Option	Description
OPSEC_SSLCA	Encryption Method: 3DES Compressed: No
OPSEC_SSLCA_COMP	Encryption Method: 3DES Compressed: Yes

7 Type the Client DN. Check Point generated this string while configuring the OPSEC Application.

8 Type the Server DN. This is the Check Point Gateway DN.

9 Click and EventTracker displays the Open window. Select the SSLCA file and then click **Open**. EventTracker populates the SSLCA file field

10 Type the Server IP. This is the IP of the host where Check Point is installed.

11 Type the Server Port. This can any port but should be consistent with what you have entered earlier in the fwopsec.conf file.

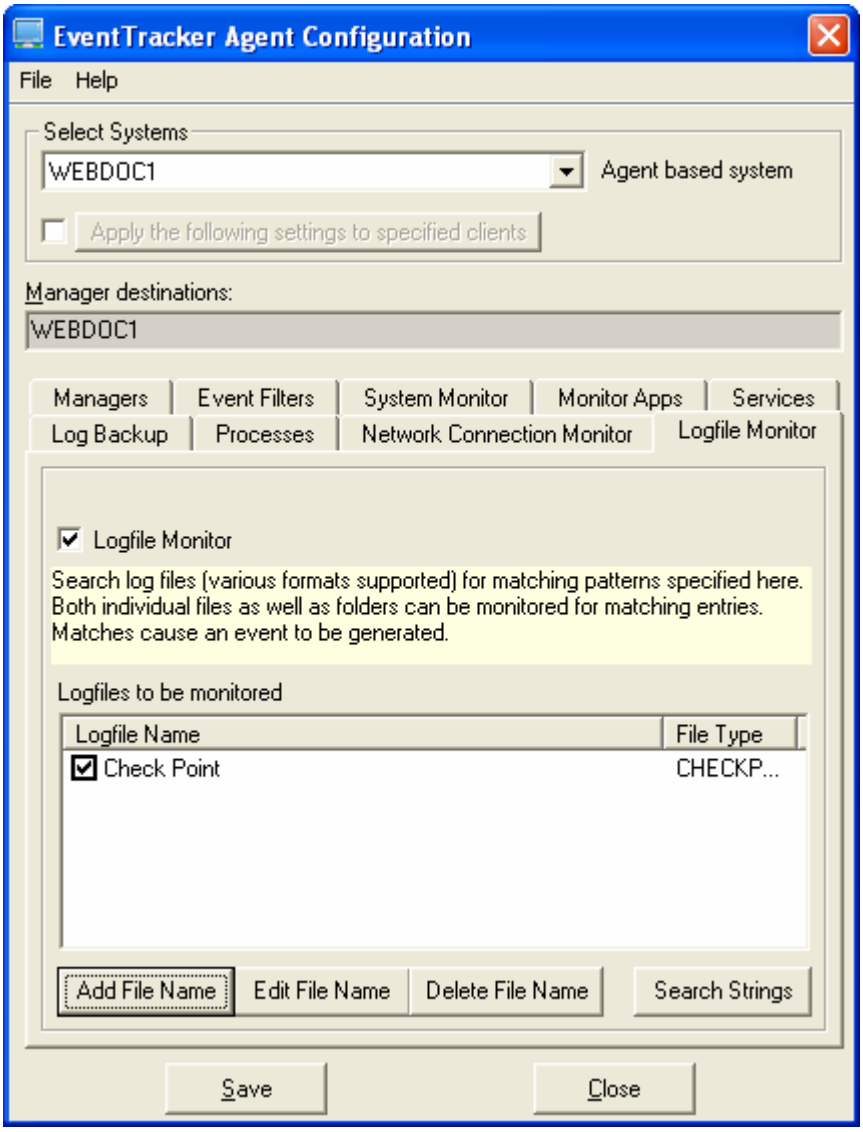
Table 46

Field	Description
Active	This option is selected by default. Select this option to receive live Check Point logs from the point in time the configuration takes affect.
Historical	Select this option to read from previous logs and the current logs as well. This option has two modes namely **Current Logs** and **All Logs**. Select the Current Logs option to read from the first record of the current log. This mode is selected by default. Select the All Logs option to read from all the backed up logs and the current logs.

12 Click **OK**.

EventTracker displays the Agent Configuration window.

Figure 261
EventTracker Agent Configuration window



13 Click **Save**.

Monitoring VMware Logs

This option helps you monitor logs generated by VMware.

To monitor VMware logs

1 Open the Agent Configuration window.

2 Select the system from the **Select System** drop-down list.

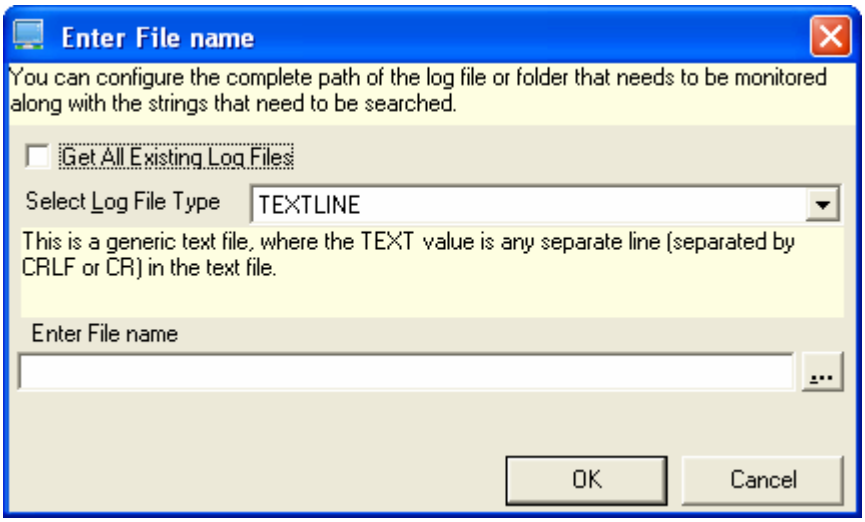
3 Click the **Logfile Monitor** tab.

EventTracker displays the Logfile Monitor tab.

4 Click **Add File Name**.

EventTracker displays the Enter File Name dialog box.

Figure 262 Enter File name dialog box


Enter File name
You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.
Get All Existing Log Files
Select Log File Type
TEXTLINE
This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.
Enter File name
OK
Cancel

5 Select the logfile type as VMWARE from the **Select Logfile Type** drop-down list.

EventTracker displays the Enter File Name dialog box.

Figure 263 Enter File Name dialog box

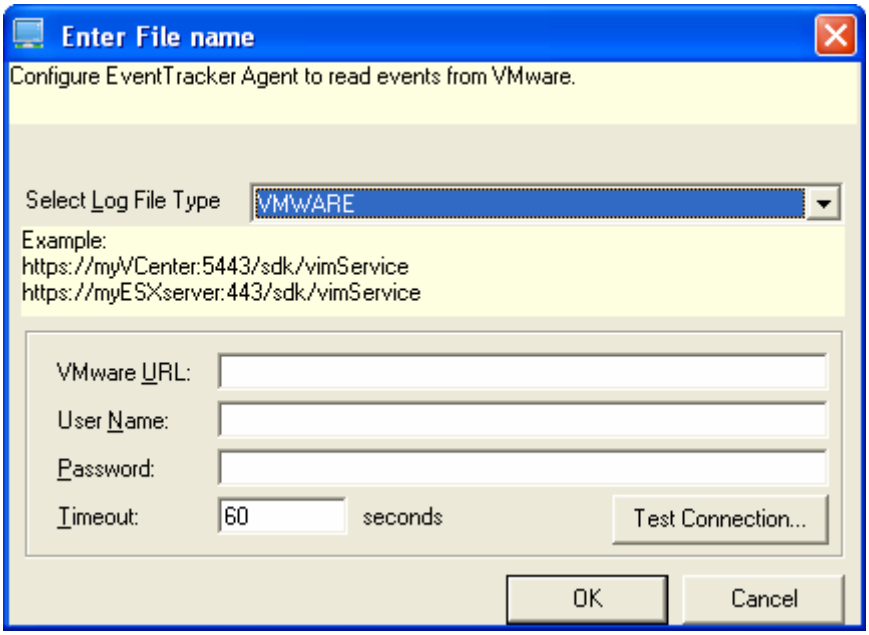


Table 47

Field	Description
VMware URL	Type a valid URL, e.g. https://esxvcserver/sdk/vimService You can also replace the server name with the IP address.
User Name	Type valid user name.
Password	Type valid password.
Timeout	Time connection timeout.

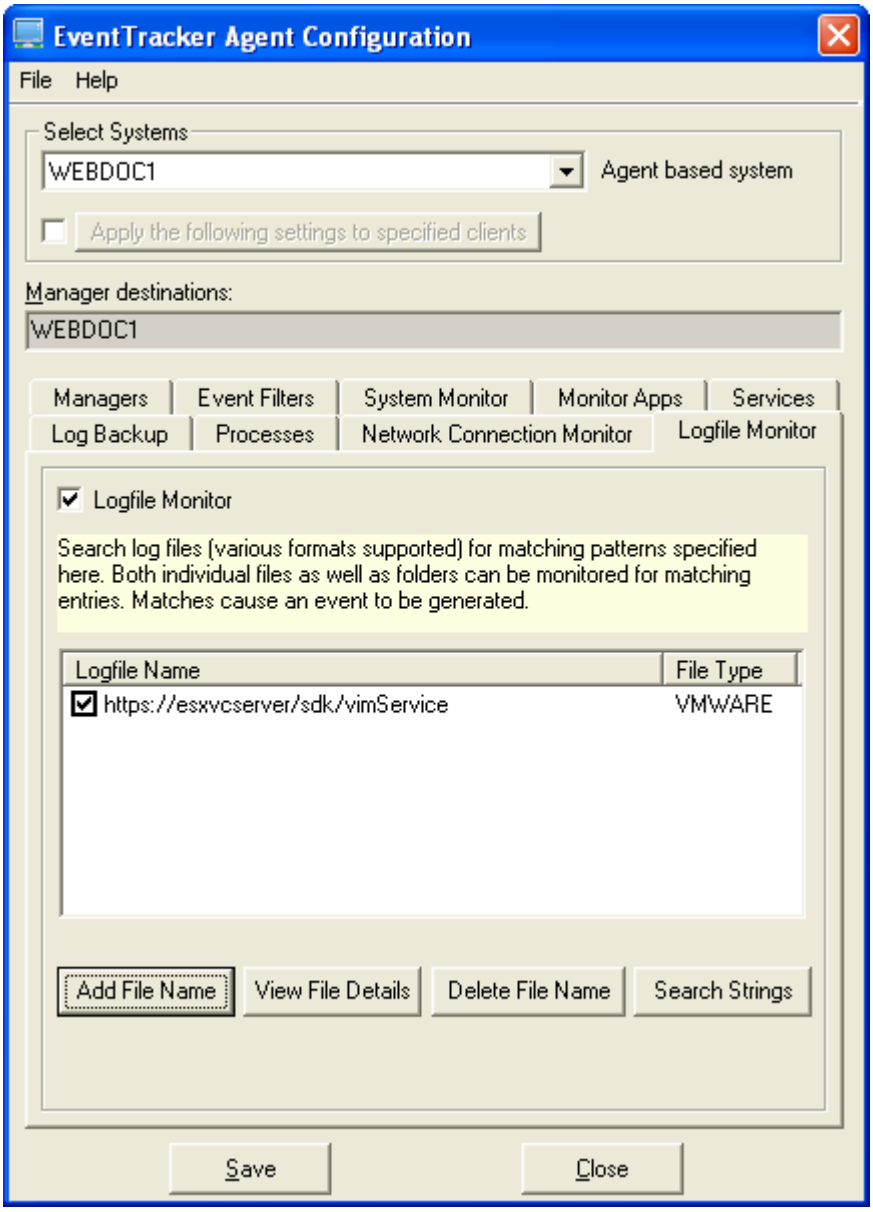
6 Type appropriately in the relevant fields.

7 Click **Test Connection** to check if the configuration parameters you have entered are correct.

8 Click **OK**.

EventTracker displays the Agent Configuration window.

Figure 264
EventTracker Agent Configuration window



9 Click **Save**.

Monitoring Network Connections

NCM provides you with the capability to effectively monitor for network connections on any system in your enterprise. It is a feature that provides you security beyond the firewall by detecting threats from inside the firewall as well as keeping the external attackers at bay.

It helps you keep track of various happenings like connections established by remote applications, unauthorized connections to server and connections made to standard ports.

NCM provides second level security beyond firewall. NCM can drastically reduce internal security threats and can be configured to raise an alert whenever any intruder outside a list of trusted IP addresses attempts to make network connection. The NCM functionality can also be set at high security mode wherein an event is generated for all incoming and out going connections.

The NCM functionality facilitates to achieve the following key objectives:

- Host based intrusion detection.
- To provide second level security and complement to firewall and anti-virus.
- In strengthening security policies.
- To improve security policies against inside security breaches.
- To monitor all network connections (TCP and UDP)
- For constant unattended, reliable monitoring of intrusion detection.
- Flexible configuration as per the business requirement.

To monitor network connections

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Network Connection Monitor** tab.

   EventTracker displays the Network Connection Monitor tab.

Figure 265 Agent Configuration window – Network Connection Monitor tab

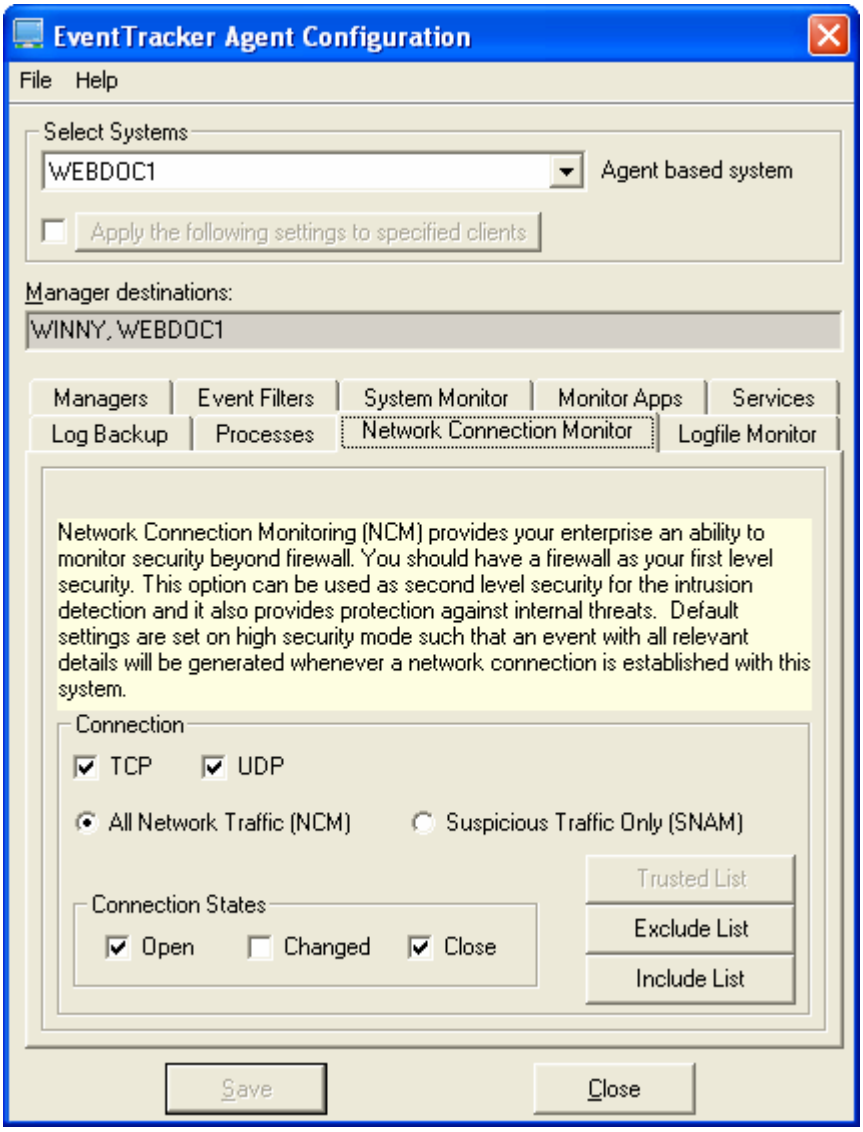

EventTracker Agent Configuration
File Help
Select Systems
WEBDOC1
Agent based system
Apply the following settings to specified clients
Manager destinations:
WINNY, WEBDOC1
Managers
Event Filters
System Monitor
Monitor Apps
Services
Log Backup
Processes
Network Connection Monitor
Logfile Monitor
Network Connection Monitoring (NCM) provides your enterprise an ability to monitor security beyond firewall. You should have a firewall as your first level security. This option can be used as second level security for the intrusion detection and it also provides protection against internal threats. Default settings are set on high security mode such that an event with all relevant details will be generated whenever a network connection is established with this system.
Connection
TCP
UDP
All Network Traffic (NCM)
Suspicious Traffic Only (SNAM)
Trusted List
Exclude List
Include List
Connection States
Open
Changed
Close
Save
Close

Table 48

Field	Description
TCP	This check box is selected by default to monitor TCP network connections.
UDP	This check box is selected by default to monitor UDP network connections.
Connection States	
Open	This check box is selected by default to monitor opened TCP/UDP connections.
Changed	Select this check box to monitor TCP/UDP connections whose

Field	Description
	connection state has been changed recently.
Close	This check box is selected by default to monitor closed TCP/UDP connections.
All Network Traffic (NCM): By default, EventTracker selects this option.	
Exclude List	Click this button to configure the network connections that need not be monitored.
Include List	Click this button to configure the network connections to monitor. Include Network Connections List always override the Exclude Network Connections List.
Suspicious Traffic Only (SNAM)	
Trusted List	Click this button to view and configure trusted network connections.

4 Select or clear **TCP** or **UDP** check box.

5 Click **Save**.

Excluding Network Connections from monitoring

To configure network connections that need not be monitored

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

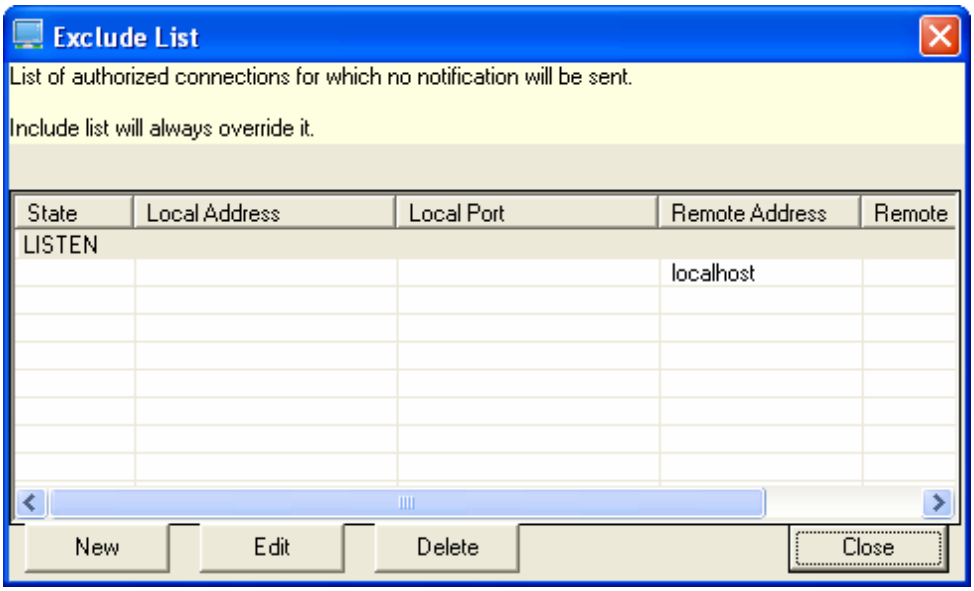
3 Click the **Network Connection Monitor** tab.

EventTracker displays the Network Connection Monitor tab.

4 Click **Exclude List**.

EventTracker displays the Exclude List dialog box.

Figure 266 Exclude List window



5 Click **New**.

EventTracker displays the Network Connection Details dialog box.

Figure 267 Network Connection Details window

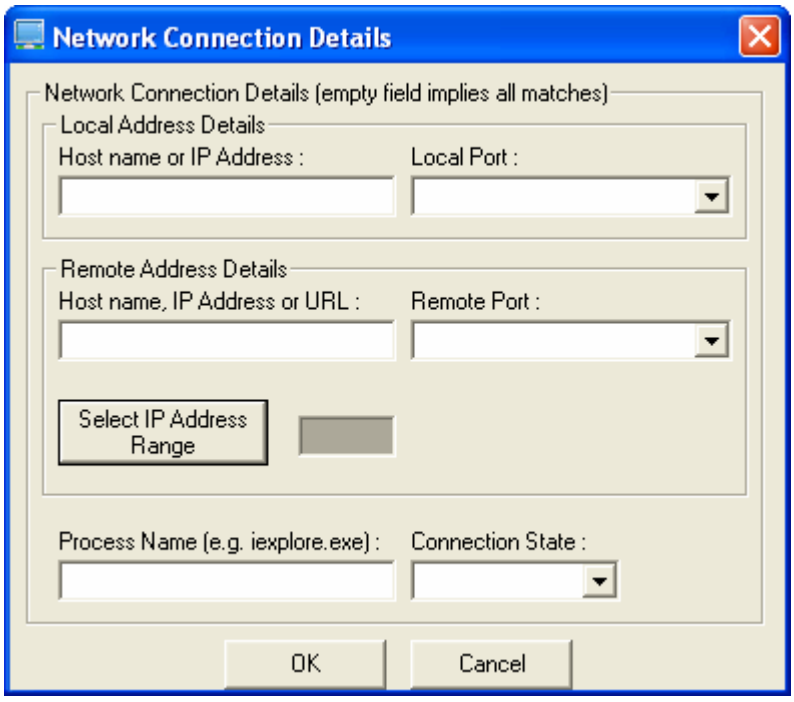
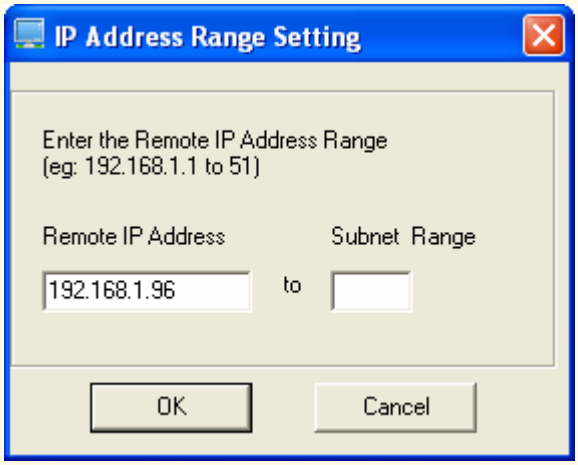


Table 49

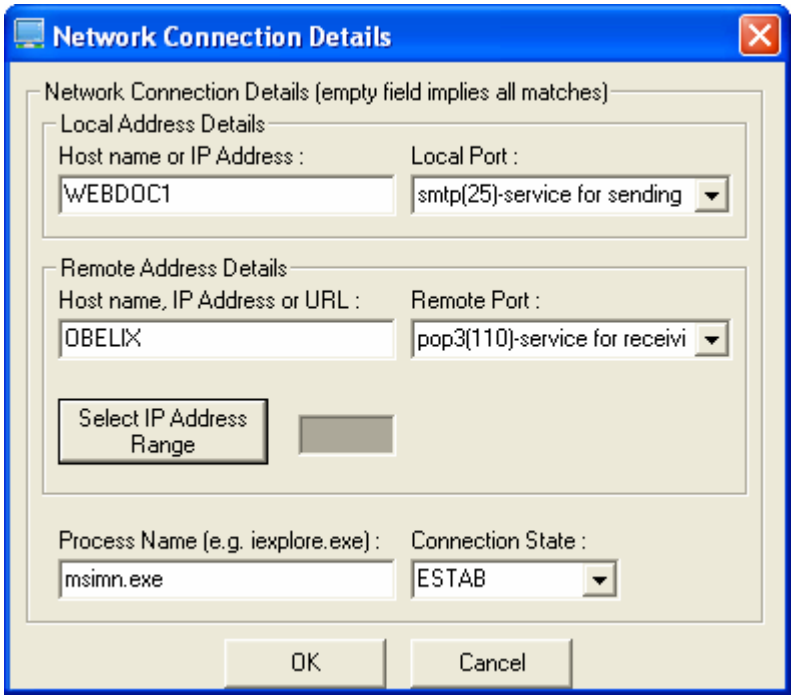
Field	Description
Local Address Details	
Host Name or IP Address	Type the host name or the IP address in this field.
Local Port	Select a local port from the drop-down list.
Remote Address Details	
Host name, IP Address or URL	Type the host name, IP address or URL in this field.
Remote Port	Select a remote port from the drop-down list.
Select IP Address Range	Click this button to add IP address range. EventTracker displays the IP Address Range Setting dialog box.  Type the range until which you want to monitor the IP network connections. This option is available only when you Type the IP address in the Host name, IP address or URL field.
Process Name	Type the process name in this field.
Connection State	Select a connection state from the drop-down list.

Note

If a field is left blank, a wildcard match for that field is assumed. For example, leaving the Local Port field blank implies that any value in that field is acceptable.

6 Type appropriately in the relevant fields.

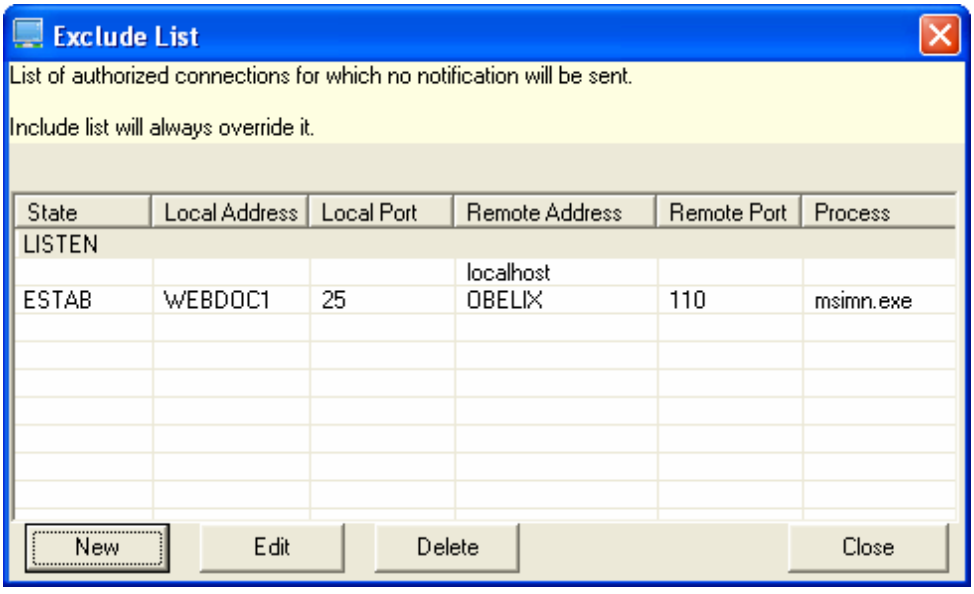
Figure 268 Network Connection Details window



7 Click **OK**.

EventTracker displays the Exclude List dialog box.

Figure 269 Exclude List window



8 To modify the network connection details, click **Edit**. Type the information in the Network Connection Details window and then click **OK**.

9 To delete the network connection details, select the network connection details you want to delete from the list and then click **Delete**.

10 Click **Close** on the Exclude List dialog box.

11 Click **Save** on the Agent Configuration window.

Including Network Connections for monitoring

To configure network connections to monitor

1 Open the Agent Configuration dialog box.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Network Connection Monitor** tab.

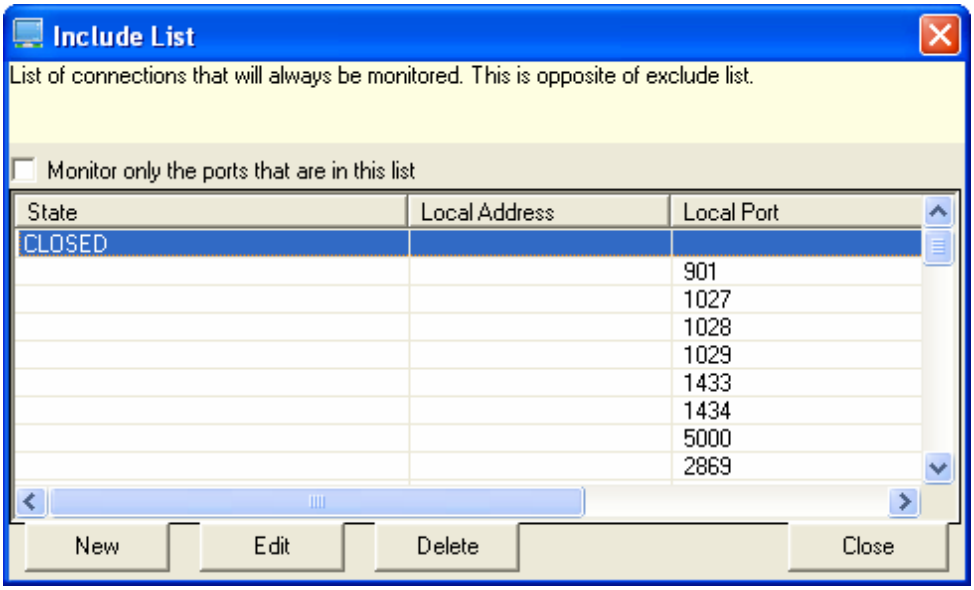
EventTracker displays the Network Connection Monitor tab.

4 Select the appropriate check boxes.

5 Click **Include List**.

EventTracker displays the Include List dialog box.

Figure 270 Include List window



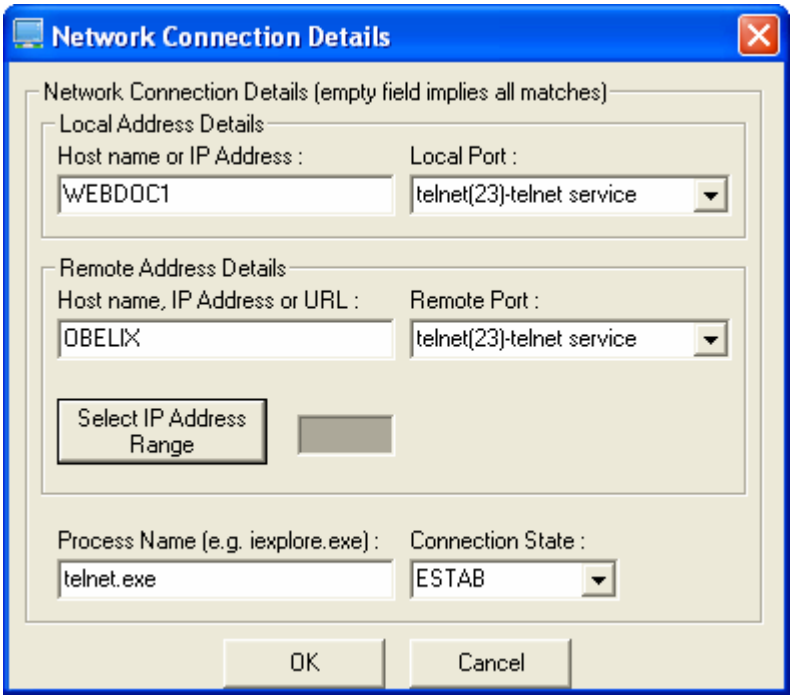
6 Select the **Monitor only the ports that are in this list** option, to monitor only the ports in the list, and then click **Close**.

7 To add more Network Connection details, click **New**.

EventTracker displays the Network Connection Details dialog box.

8 Type appropriately in the relevant fields.

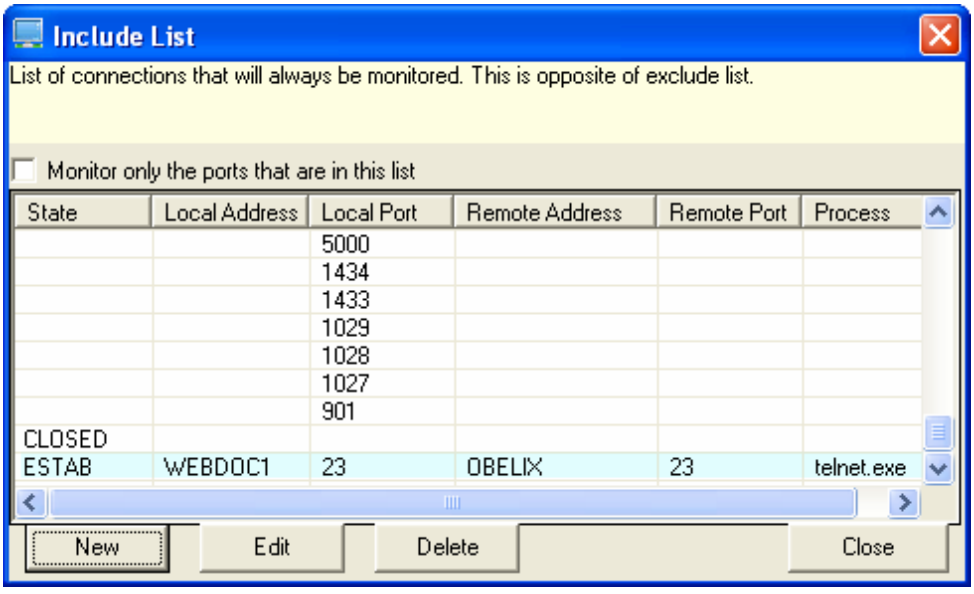
Figure 271 Network Connection Details window



9 Click **OK**.

EventTracker displays the **Include List** dialog box.

Figure 272 Include List window



10 To modify the network connection details, click **Edit**. Type the information in the Network Connection Details window and then click **OK**.

11 To delete the network connection details, select the network connection details you want to delete from the list and then click **Delete**.

12 Click **Close**.

13 Click **Save** on the Agent Configuration window.

Suspicious Connections

This feature is an enhancement of the existing Network Connection Monitoring. This option enables you to monitor the suspicious usage of TCP or UDP ports and their connection states. By default, all the connections are suspicious and you can exempt applications and ports from monitoring. EventTracker is shipped along with a list of applications and ports, which are not harmful to any enterprise environment. As discussed, EventTracker Agent will not monitor these White-listed applications and ports.

Note

Prior to enabling EventTracker Agent to monitor Suspicious Traffic, apply all the latest Microsoft patches / hotfixes if the operating system is Windows 2000.

Monitoring Suspicious Connections

This option helps you to monitor suspicious connections and to view predefined trusted connections list. EventTracker does not monitor the connections listed in Trusted List. You can also edit predefined trusted connection list and define your own set of trusted connection list.

To view Trusted List

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

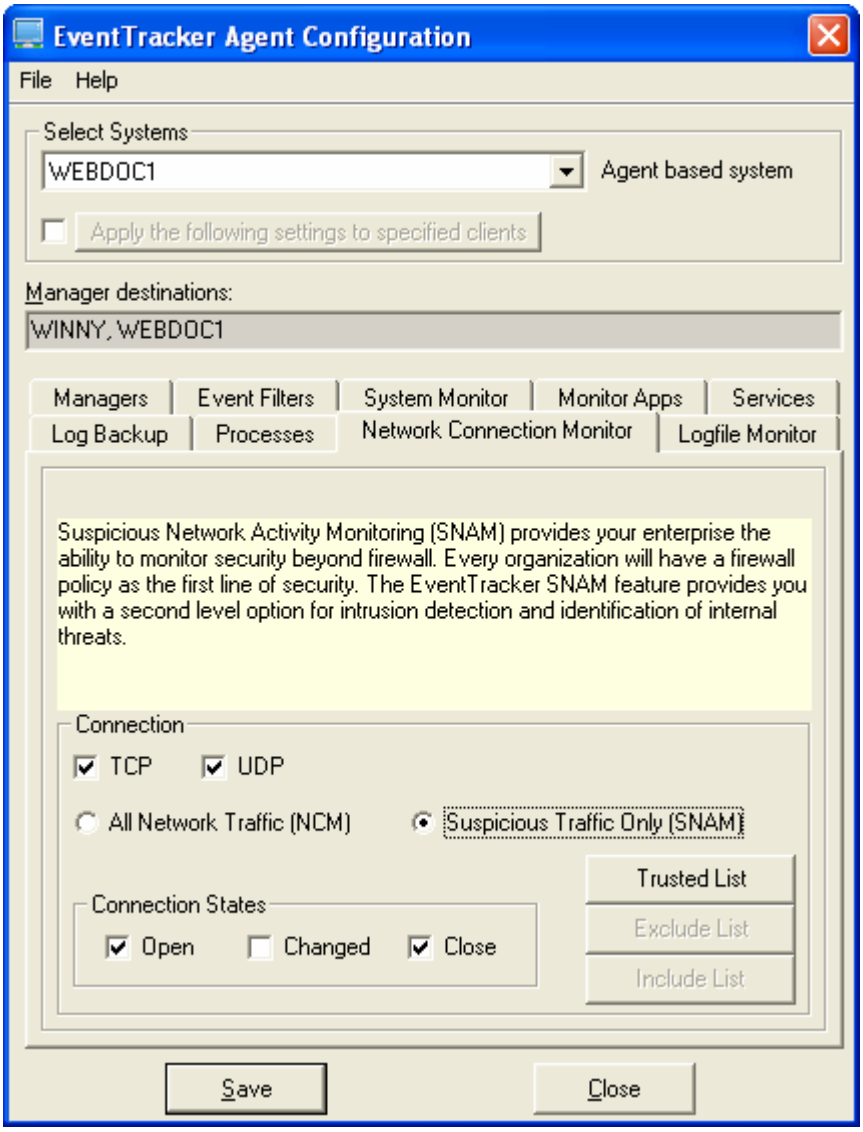
3 Click the **Network Connection Monitor** tab.

EventTracker displays the Network Connection Monitor tab.

4 Select the **Suspicious Traffic Only (SNAM)** option.

EventTracker displays the Agent Configuration window.

Figure 273 Agent Configuration window – Network Connection Monitor tab



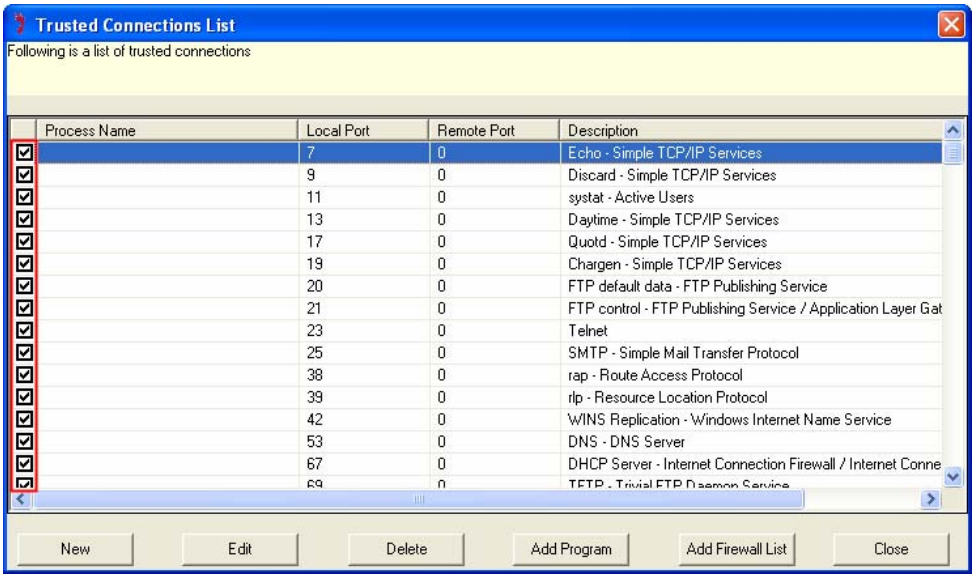
5 Click **Trusted List**.

Note

The trusted list contains a list of known good applications and ports through which the usual network connections between the processes happen. This option helps you to view, enable and disable predefined trusted connections list. EventTracker exempts enabled connections listed in Trusted List from monitoring. You can also edit predefined trusted connection list and define your own set of trusted connection list.

EventTracker displays the Trusted Connections List. The connections listed in the Trust List are exempted from monitoring.

Figure 274 Trusted Connections List

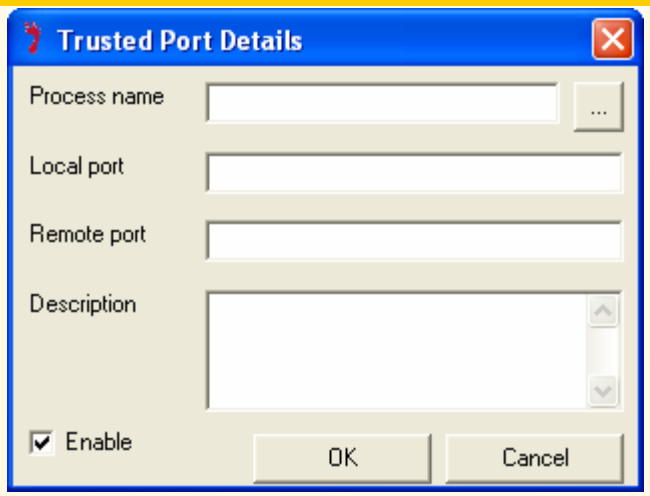
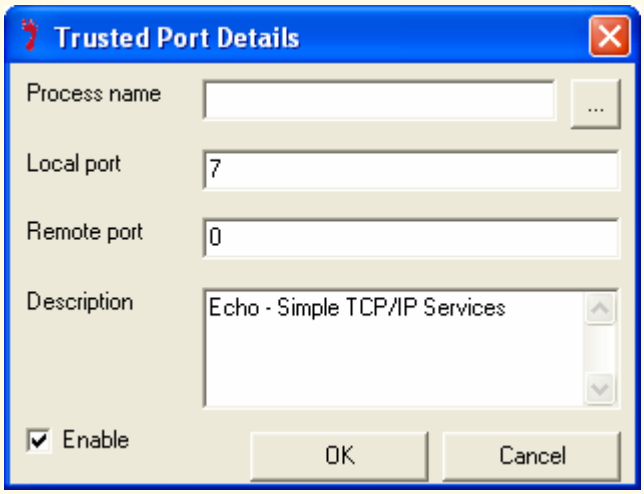

Trusted Connections List
Following is a list of trusted connections
Process Name
Local Port
Remote Port
Description
7 0 Echo - Simple TCP/IP Services
9 0 Discard - Simple TCP/IP Services
11 0 systat - Active Users
13 0 Daytime - Simple TCP/IP Services
17 0 Quotd - Simple TCP/IP Services
19 0 Chargen - Simple TCP/IP Services
20 0 FTP default data - FTP Publishing Service
21 0 FTP control - FTP Publishing Service / Application Layer Gat
23 0 Telnet
25 0 SMTP - Simple Mail Transfer Protocol
38 0 rap - Route Access Protocol
39 0 rlp - Resource Location Protocol
42 0 WINS Replication - Windows Internet Name Service
53 0 DNS - DNS Server
67 0 DHCP Server - Internet Connection Firewall / Internet Conne
New
Edit
Delete
Add Program
Add Firewall List
Close

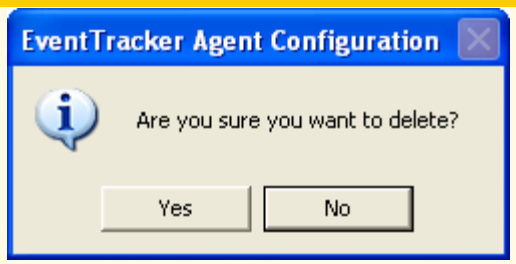
Note

By default, the predefined trusted connections are enabled, which means EventTracker exempts those processes and ports from monitoring. Clear the check boxes against the processes that you want to be monitored by EventTracker.

Table 50

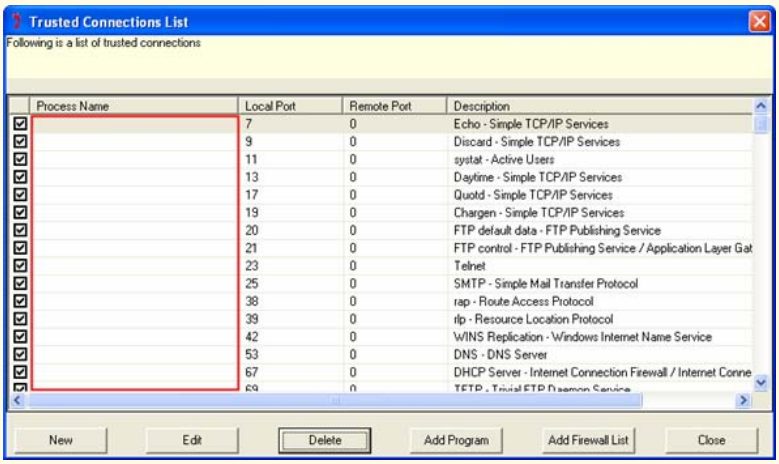
Click	To
New	Add new trusted connections. EventTracker displays Trusted Port Details window.

Click	To
	 Type appropriate details in the relevant fields and then click **OK**. You can use wild cards to search processes. For example, had you configured Virtual Collection Points and wish to add all EventTracker Receiver processes, it is enough to provide the Process name as EtReceiver*.exe. You can also use browse button to locate the process.
Edit	Select a process from the list and then click **Edit**. EventTracker displays Trusted Port Details window.  Edit details in the relevant fields and then click **OK**.
Delete	Select a process from the list and then click **Delete**. EventTracker displays confirmation message box.

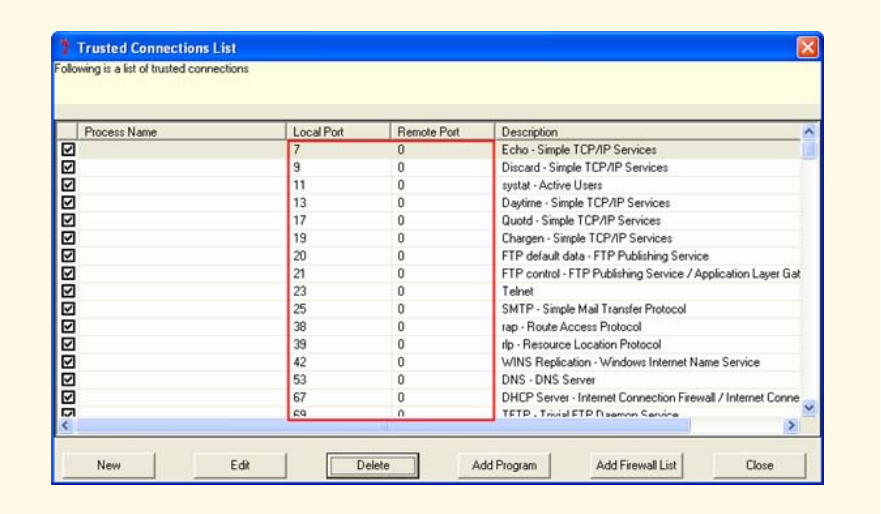
Click	To
	 Click Yes to delete the selected entry.
Add Program	Add programs installed in your computer to the trusted list.
Add Firewall List	Add programs included in the Firewall Exceptions list to the trusted list.
Close	Close the Trusted Suspicious Connections List window.

Note

In some rows in the list, you might notice **Process Name** field is empty, this signifies that any process that communicate through the defined ports are deemed to be legitimate.


Trusted Connections List
Following is a list of trusted connections
Process Name
Local Port
Remote Port
Description
7 0 Echo - Simple TCP/IP Services
9 0 Discard - Simple TCP/IP Services
11 0 systat - Active Users
13 0 Daytime - Simple TCP/IP Services
17 0 Quotd - Simple TCP/IP Services
19 0 Chargen - Simple TCP/IP Services
20 0 FTP default data - FTP Publishing Service
21 0 FTP control - FTP Publishing Service / Application Layer Gat
23 0 Telnet
25 0 SMTP - Simple Mail Transfer Protocol
38 0 rap - Route Access Protocol
39 0 rlp - Resource Location Protocol
42 0 WINS Replication - Windows Internet Name Service
53 0 DNS - DNS Server
67 0 DHCP Server - Internet Connection Firewall / Internet Conne
New
Edit
Delete
Add Program
Add Firewall List
Close

Similarly, in some rows you might notice that the Local and Remote ports are 0 (zero). This signifies that the processes listed could use any available ports to communicate. EventTracker considers that traffic to be legitimate and exempts from monitoring.


Trusted Connections List
Following is a list of trusted connections
Process Name
Local Port
Remote Port
Description
7 0 Echo - Simple TCP/IP Services
9 0 Discard - Simple TCP/IP Services
11 0 systat - Active Users
13 0 Daytime - Simple TCP/IP Services
17 0 Quotd - Simple TCP/IP Services
19 0 Chargen - Simple TCP/IP Services
20 0 FTP default data - FTP Publishing Service
21 0 FTP control - FTP Publishing Service / Application Layer Gat
23 0 Telnet
25 0 SMTP - Simple Mail Transfer Protocol
38 0 rap - Route Access Protocol
39 0 rlp - Resource Location Protocol
42 0 WINS Replication - Windows Internet Name Service
53 0 DNS - DNS Server
67 0 DHCP Server - Internet Connection Firewall / Internet Conne
New
Edit
Delete
Add Program
Add Firewall List
Close

Adding programs to the trusted list

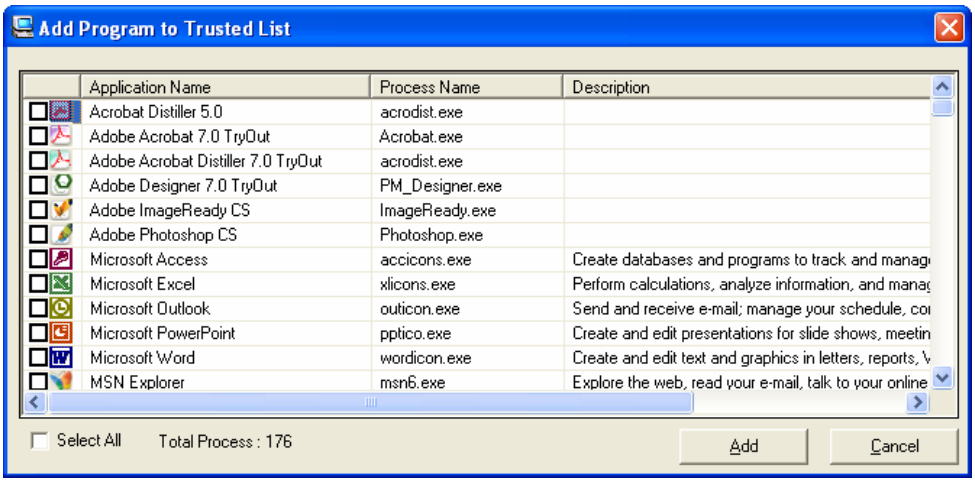
This option helps you add programs installed in your computer to the trusted list. You can enable or disable the entries in the trusted programs list. Enable means the processes and the ports used by the processes are legitimate and disable means illegitimate and EventTracker monitors them.

To add programs to the trusted list

1. Click **Add Program**.

   EventTracker displays the Add Program to Trusted List window.

Figure 275 Add Program to Trusted List window


Add Program to Trusted List
Application Name
Process Name
Description
Acrobat Distiller 5.0 acrodist.exe
Adobe Acrobat 7.0 TryOut Acrobat.exe
Adobe Acrobat Distiller 7.0 TryOut acrodist.exe
Adobe Designer 7.0 TryOut PM_Designer.exe
Adobe ImageReady CS ImageReady.exe
Adobe Photoshop CS Photoshop.exe
Microsoft Access accicons.exe Create databases and programs to track and manag
Microsoft Excel xlicons.exe Perform calculations, analyze information, and manag
Microsoft Outlook outicon.exe Send and receive e-mail; manage your schedule, co
Microsoft PowerPoint pptico.exe Create and edit presentations for slide shows, meetin
Microsoft Word wordicon.exe Create and edit text and graphics in letters, reports, V
MSN Explorer msn6.exe Explore the web, read your e-mail, talk to your online
Select All
Total Process : 176
Add
Cancel

2 Select the check box against the programs or select the **Select All** check box to select all the programs.

3 Click **Add**.

EventTracker adds the selected program to the Trusted Connections List.

4 Click **Close**.

5 Click **Save** on the Agent Configuration window.

Adding Firewall Exceptions to the Trusted List

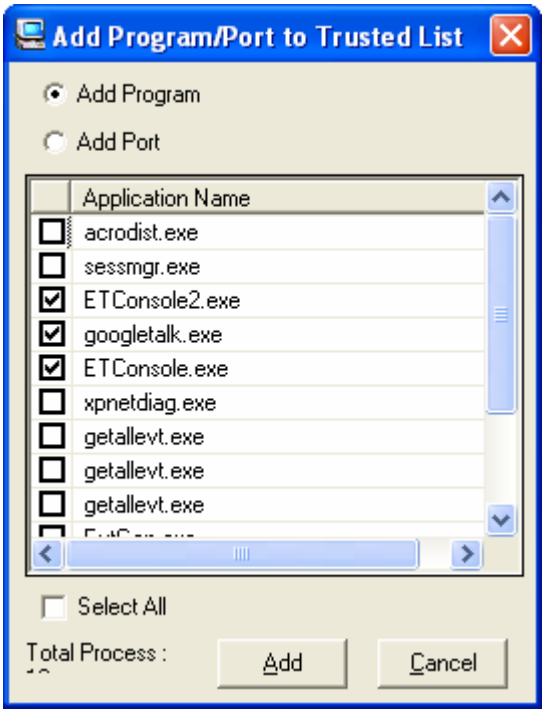
This option helps you add the processes and ports in the Firewall programs and ports Exceptions to the trusted list.

To add Firewall Exceptions to the Trusted List

1 Click **Add Firewall List**.

EventTracker displays the Add Program/Port to Trusted List window.

Figure 276 Add Program/Port Trusted List window

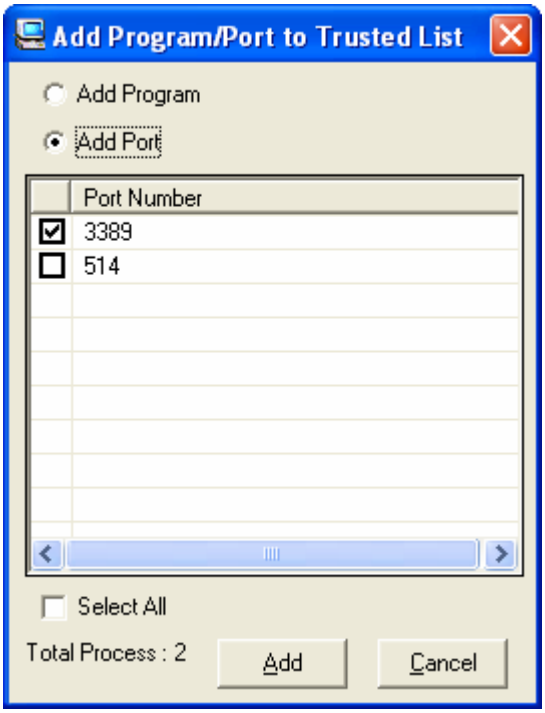


By default, EventTracker selects the **Add Program** option and displays the programs in the exceptions list.

2 Select the **Add Port** option.

EventTracker displays the Add Program/Port to Trusted List window.

Figure 277 Add Program/Port Trusted List window



3 Select the programs or select the **Select All** check box and then click **Add** to add programs to the trusted list.

EventTracker adds the selected items to the Trusted Connections List.

Monitoring Processes

Process monitoring enables the administrator to keep tabs on the general health of processes on a system. You can configure general process health thresholds for CPU and Memory Usage per process. CPU usage is measured in terms of percentage while Memory usage is measured in absolute terms.

When the configured threshold is crossed, an event will be generated and reported to the Manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. So, when an event is seen that a process is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

By default, all processes will be monitored and the default threshold limits are 80MB of Memory Usage and 60% of CPU.

You can also choose to filter out processes that you do not want to monitor. By default, all processes will be monitored.

To configure the process to monitor

1. Open the Agent Configuration window.
2. Select the system from the **Select Systems** drop-down list.
3. Click the **Processes** tab.

   EventTracker displays the Processes tab.

Figure 278 Agent Configuration window – Processes tab

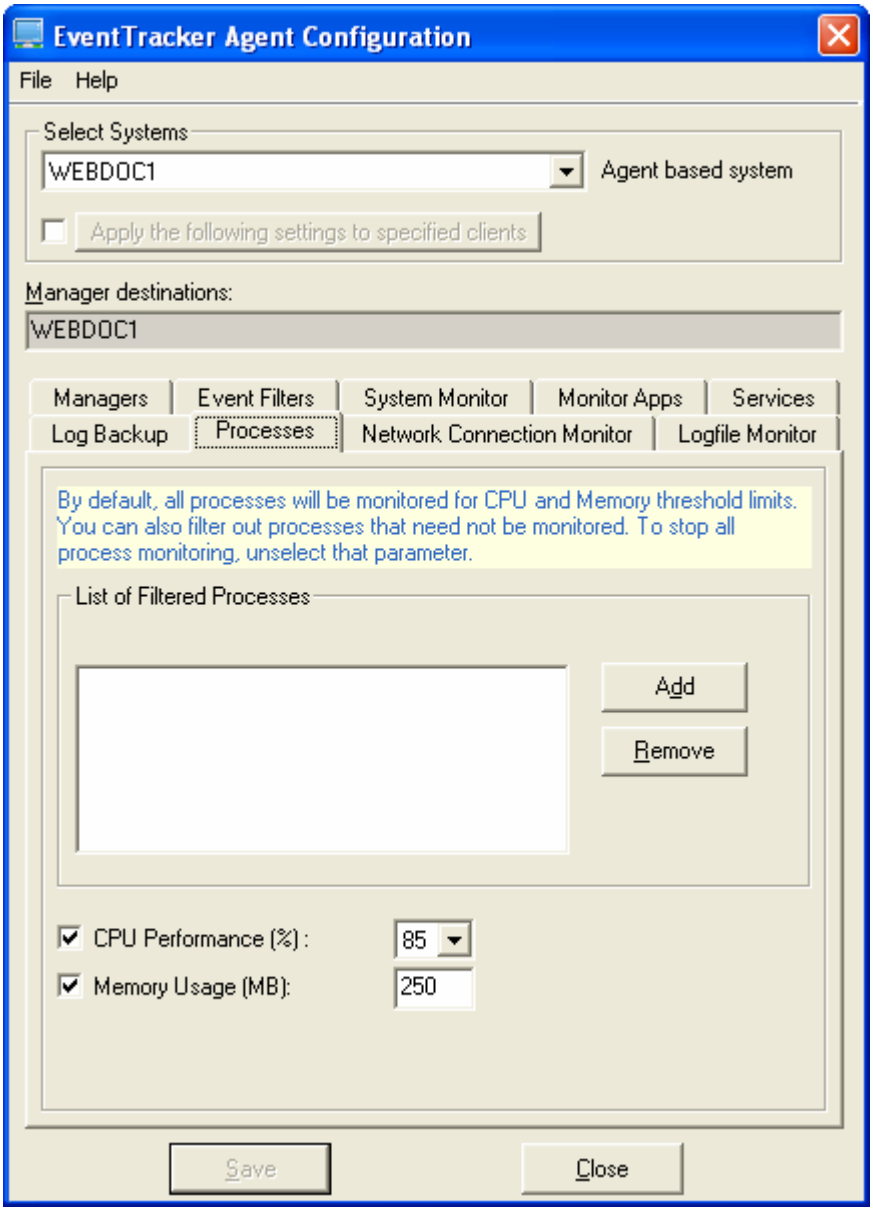


Table 51

Field	Description
CPU Performance (%)	Select CPU Performance threshold limit from the drop-down list.
Memory Usage (MB)	Type the Memory Usage threshold limit in MB in this field.

4 Click **Add**.

EventTracker displays the EventTracker Agent Configuration dialog box.

5 Type the process name in the **Enter Process Name** field.

6 Click **OK**.

EventTracker adds the process to the List of Filtered Processes.

7 Click **Save** on the Agent Configuration window.

Note

EventTracker generates the process event when the set threshold value crosses the limit for more than 3 minutes.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 286.

Removing processes from List of Filtered Processes

To remove processes from List of Filtered Processes

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Processes** tab.

EventTracker displays the Processes tab.

4 Select the process you do not want to monitor from the **List of Filtered Processes** list.

5 Click **Remove**.

EventTracker displays the EventTracker Agent Configuration confirmation message box.

6 Click **Yes**.

EventTracker removes the selected process.

Click **Save** on the Agent Configuration window.

Maintaining Log Backup

This option enables you to backup event logs automatically in the EventTracker Agent directory whenever the event logs are full. EventTracker automatically performs event log backup or archival in the standard Windows event log format (`.evt` / `.evtx` format).

To backup event logs automatically

1 Open the Agent Configuration window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Log Backup** tab.

EventTracker displays the Log Backup tab.

Figure 279 Agent Configuration window – Log Backup tab

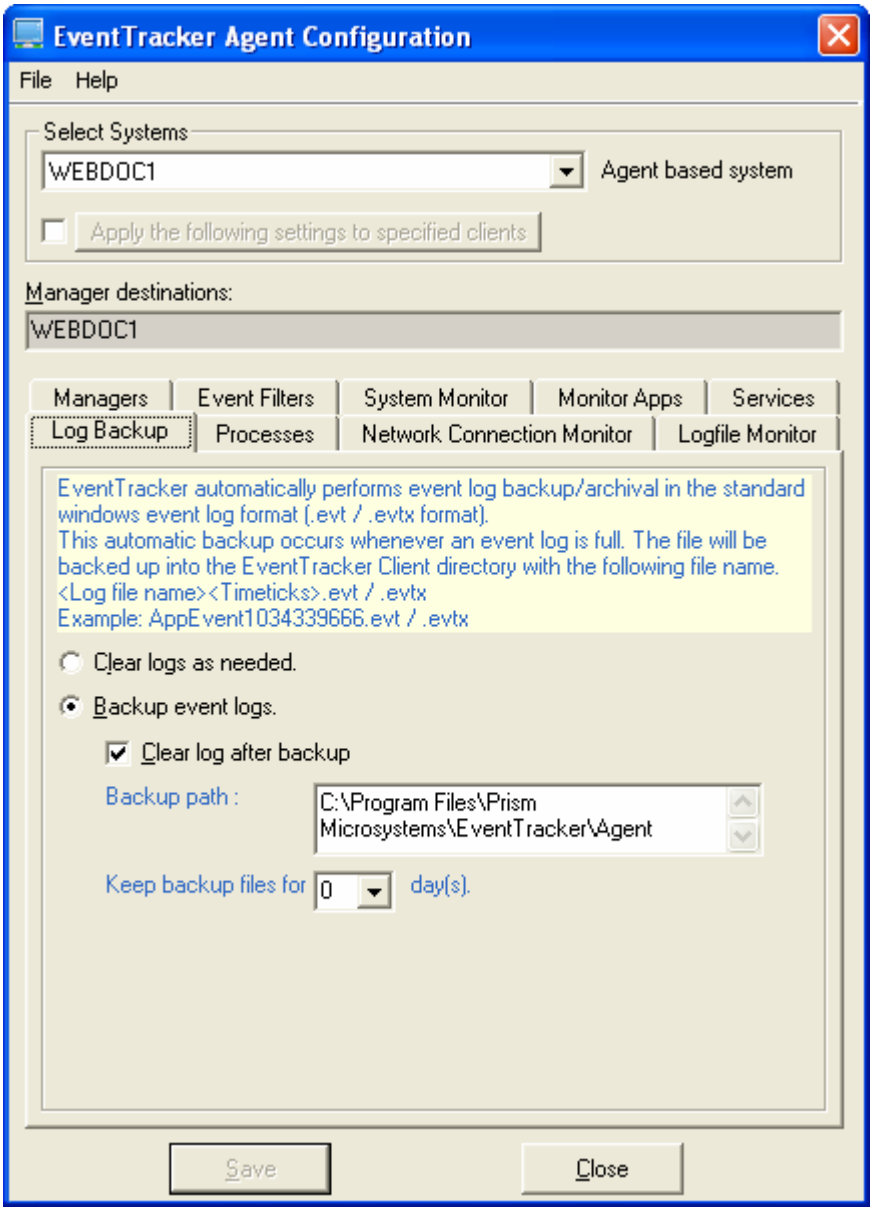


Table 52

Field	Description
Clear logs as needed	If selected, EventTracker Agent clears log file if and only if offset error is encountered. After clearing, Agent inserts "3241" event to notify the user. In this case, no backup is taken. This is true for any setting of the Windows Event Log's "When maximum log size is reached" option (i.e. Overwrite events as needed, Overwrite events older than N days, Do not overwrite events (clear log manual)) EventTracker log backup and clear operation:

Field	Description
	Computer: EXCHTEST Log file name: Application Log file backup: Not applicable Log file clear: Success Reason: Received invalid offset error while reading the event log. For more information see Microsoft KB Article #177199.
Backup event logs	If the "Backup event logs" option is selected, and If the offset is lost at any point, no matter whether "Clear log after backup" check box is selected or not the respective log file will be backed up and cleared and the following 3241 event will be logged. EventTracker log backup and clear operation: Computer: EXCHTEST Log file name: Security Log file backup: C:\Program Files\Prism Microsystems\EventTracker\Agent\ EXCHTEST\ Eventlog_Backup_Security1221683647.evt Log file clear: Success Reason: Invalid offset error while reading the event log. For more information see Microsoft KB Article #177199.
Backup Path	By default backed up log files are stored in the EventTracker installation folder typically, …\Program Files\Prism Microsystems\EventTracker\Agent You cannot change this path.
Keep backup files for	If selected, backup files older than selected number of days will be automatically deleted by the agent.

4 Select the options appropriately and then click **Save** on the Agent Configuration window.

You can apply the current settings to other specified Agents. For more information, refer Applying Configuration Settings to Specified Agents on page 285.

Viewing Logs

This option enables you to view the log details.

To view the log details

1 Open the System Manager.

2 Click the **View** menu and select the **Log** option.

EventTracker displays log details in the Notepad.

Applying Configuration Settings to Specified Agents

This option enables you to apply the current configuration settings of the selected system to other specified Agents from one centralized location.

To apply configuration settings to specified Agents

1. Open the Agent Configuration window.

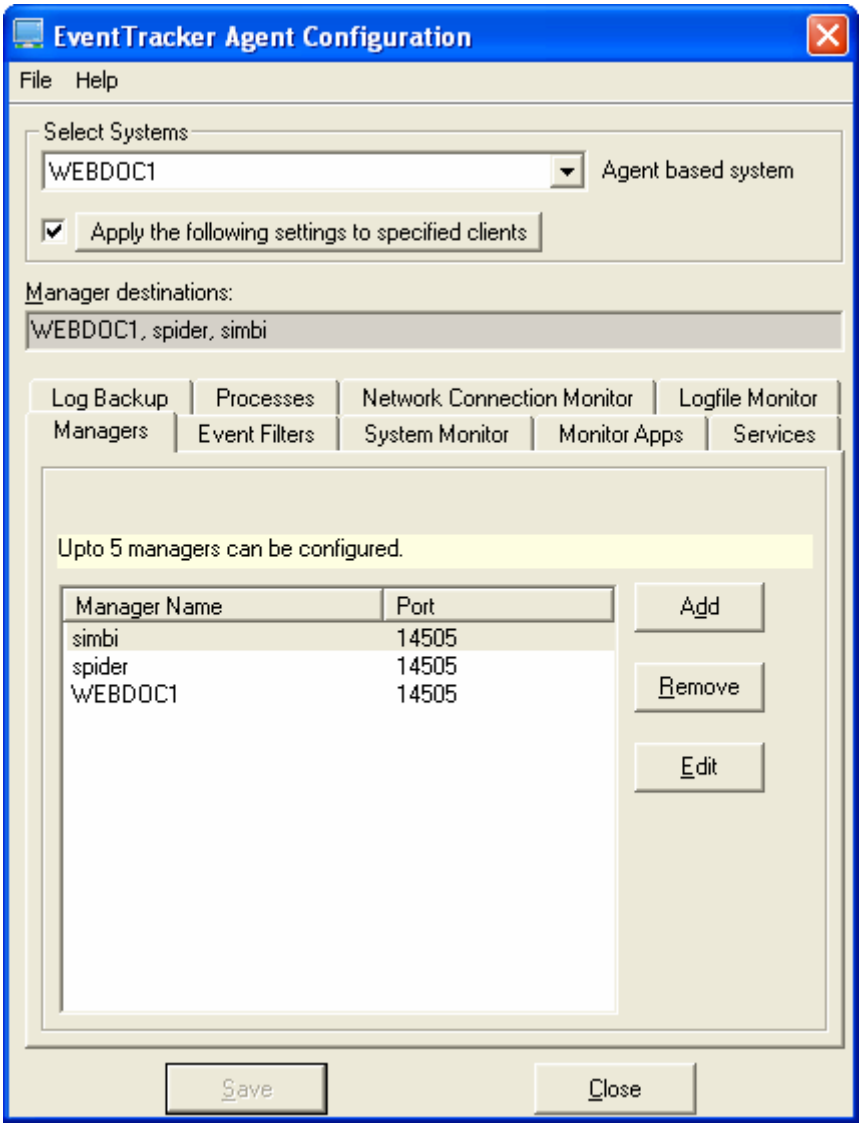
   EventTracker, by default displays the Managers tab.

2. Select the system from the **Select Systems** drop-down list.

> **Note**
>
> Only the saved configuration settings can apply to the specified Agents.

3. Select the check box next to **Apply the following settings to specified Agents**. EventTracker enables the button.

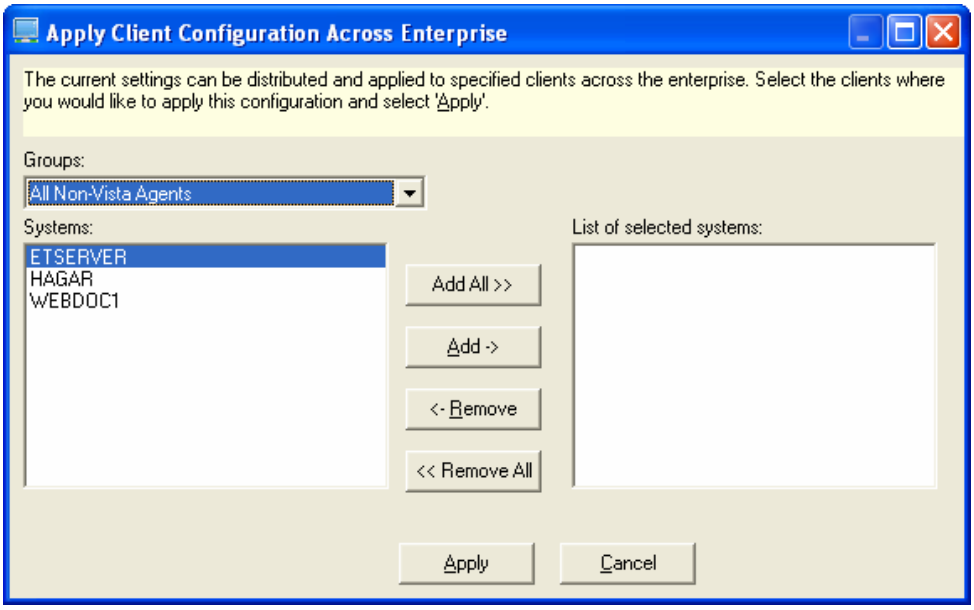
Figure 280 Agent Configuration window – Managers tab



4 Click **Apply the following settings to specified Agents**.

EventTracker displays the Apply Client Configuration Across Enterprise dialog box.

Figure 281 Apply Client Configuration Across Enterprise window



5 Select the group and computer for which you want to apply the configuration settings.

Select the **All Non-Vista Agents** option from the Groups drop-down list to view all systems where non-Vista Agents has been deployed.

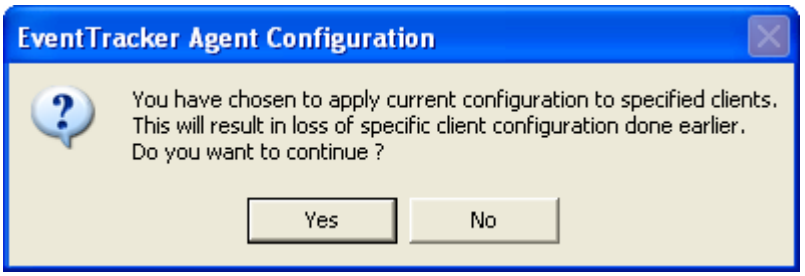
Select the **All Vista Agents** option from the Groups drop-down list to view all systems where Vista Agent has been deployed.

EventTracker displays the Apply Client Configuration Across Enterprise dialog box with the selected systems.

6 Click **Apply**.

EventTracker displays the EventTracker Agent Configuration message box.

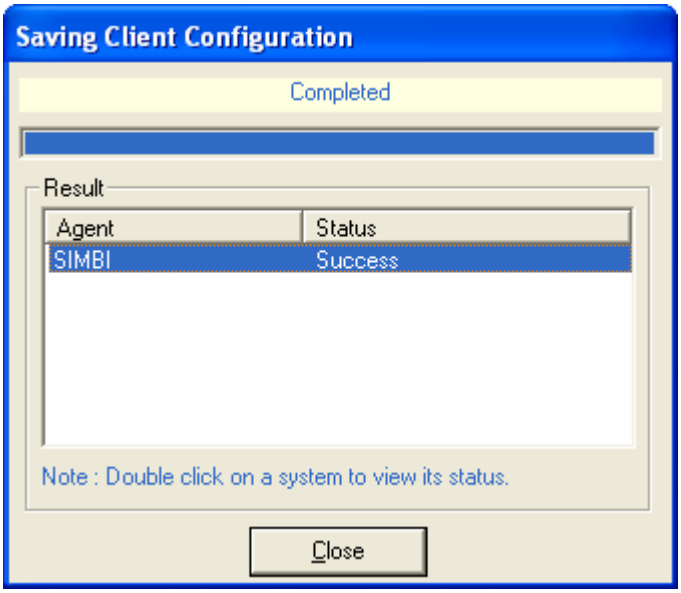
Figure 282 Apply Client Configuration Across Enterprise – message box


EventTracker Agent Configuration
You have chosen to apply current configuration to specified clients.
This will result in loss of specific client configuration done earlier.
Do you want to continue ?
Yes
No

7 Click **Yes**.

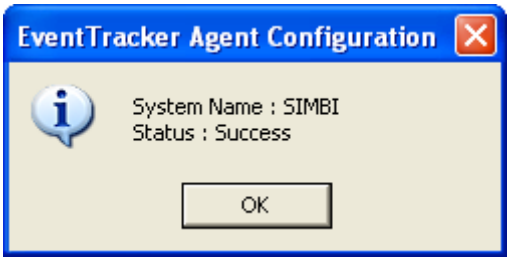
EventTracker displays the success status.

Figure 283 Saving Agent Configuration pop-up window



8 Double-click the system name. EventTracker displays EventTracker Agent Configuration message box.

Figure 284 EventTracker Agent Configuration message box



9 Click **OK**.

10 Click **Close** on the Saving Client Configuration window.

11 Click **Save**.

Backing up Current Configuration

This option enables you to back up the current configuration settings.

To back up the current configuration settings

1 Open the Agent Configuration window.

EventTracker, by default displays the Managers tab.

2 Select the system from the **Select Systems** drop-down list.

3. Click the **File** menu and click the **Backup** option.

   EventTracker, by default displays the Backup Current Configuration dialog box.

4. Select the path where you want to backup the current configuration settings.
5. Enter the file name in the **File name** field.

> **Note**
>
> The valid file extension is `.ini`

6. Click **Open**.

   EventTracker displays the EventTracker Agent Configuration message box.

7. Click **OK**.

Protecting the Current Configuration Settings

This option enables you to protect the current configuration settings.

To protect the current configuration settings for local system

1. Open the Agent Configuration window.

   EventTracker, by default displays the Managers tab.

2. Select the system from the **Select Systems** drop-down list.
3. Click the **File** menu and select the **Security** option.

   EventTracker displays the Security dialog box.

Figure 285 Security dialog box

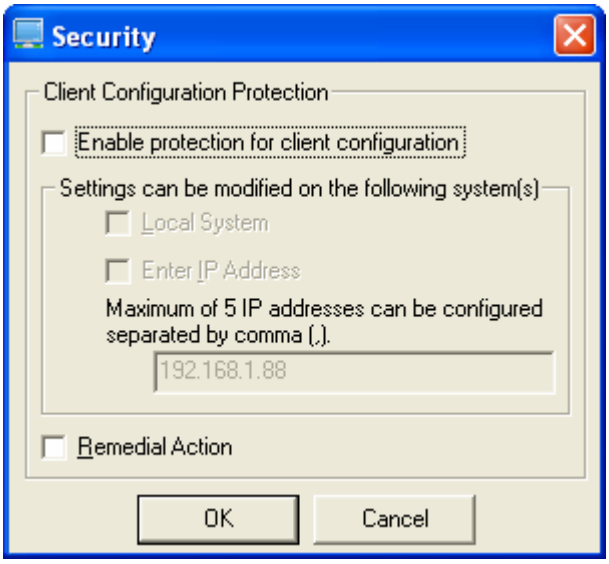


Table 53

Field	Description
Agent Configuration Protection	
Enable protection for Agent configuration	Select this check box to enable other options in this dialog box.
Settings can be modified on the following system(s)	
Local System	Select this check box to protect the current configuration settings only for the local system. Other users cannot modify your settings from their machines.
Enter IP Address	Select this check box to protect the current configuration settings for other machines. Type the IP address in the displayed dialog box. You can configure the current configuration settings up to five IP addresses.
Remedial Action	Enable Remedial Action.

4 Select the **Enable protection for Agent configuration** check box.

5 Select/enter appropriately in the relevant fields.

6 Click **OK**.

EventTracker displays the EventTracker Agent Configuration confirmation message box.

7 Click **Yes**.

Enabling Remedial Action

After enabling remedial actions at the Manager Console, you have to individually enable Remedial Action on all the Agent systems. You can also include or exclude Agents from taking remedial actions.

1. Open the Management Console.
2. Click the **Configure** menu and then select the **Configure Agents** option.
3. Select a system where you want to execute remedial actions from the **Select Systems** drop-down list.
4. Click the **File** menu and then select the **Security** option.

   EventTracker displays the Security window.
5. Select the **Remedial Action** check box.
6. Click **Save**.
7. Click **Close**.

Windows Agent Management Tool

Agent Management Tool is a diagnostic tool to check the healthy status of remote agents, restart the failed agent services and to check the version of remote agents. You ought to have Domain Admin privilege to use this utility.

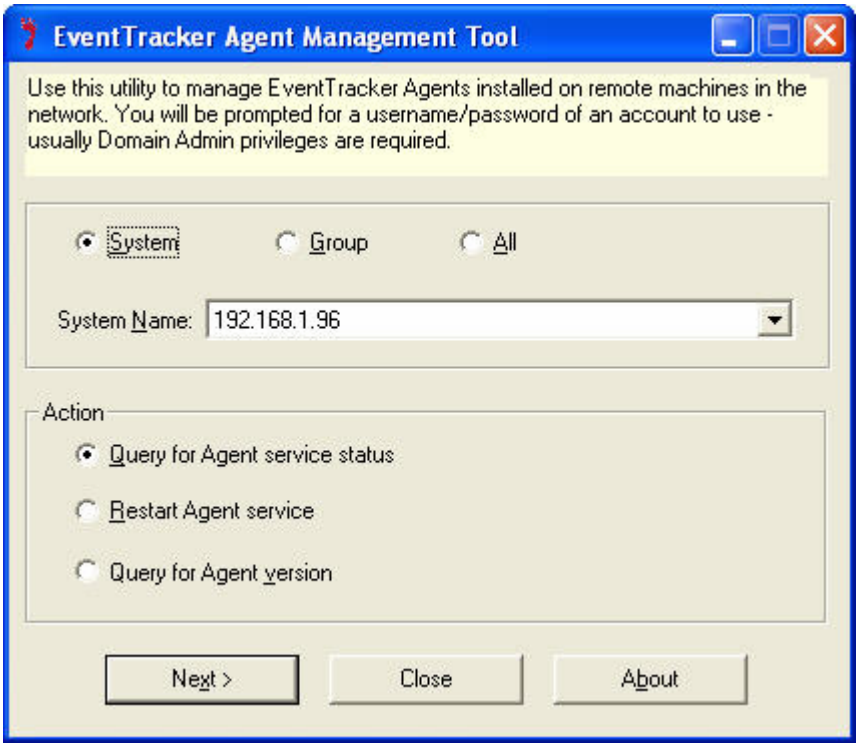
Accessing Agent Management Tool

To access the Agent Management Tool

1. Open the System Manager.
2. Click the **Options** menu and select the **Agent Management Tool** option.

   EventTracker displays the Agent Management Tool.

Figure 286 Agent Management Tool


EventTracker Agent Management Tool
Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.
System
Group
All
System Name:
192.168.1.96
Action
Query for Agent service status
Restart Agent service
Query for Agent version
Next >
Close
About

Querying Agent Service status - System

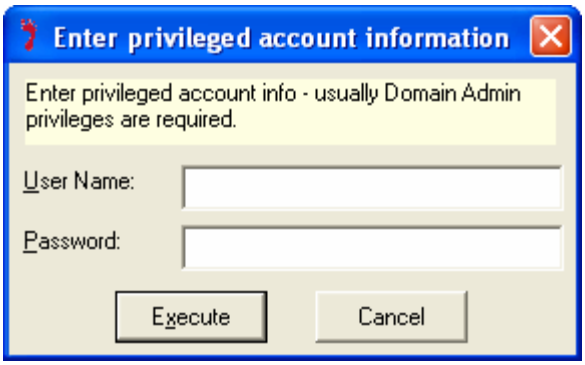
This option enables you to query agent service status in the selected system.

To query agent service status in the selected system

1. Select the **System** option, which is selected by default.
2. Select the system from the **System Name** drop-down list.
3. Select the **Query for Agent service status** option, which is selected by default.
4. Click **Next >**.

   EventTracker displays the Enter Privileged account information dialog box.

Figure 287 Enter privileged account information

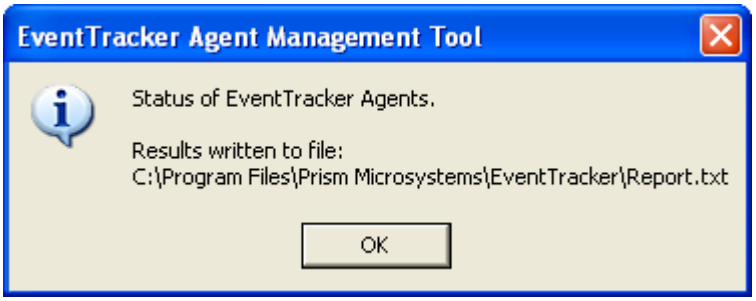


5 Type valid user name in the **User Name** text box and valid password in the **Password** text box.

6 Click **Execute**.

EventTracker displays the EventTracker Management Tool message box.

Figure 288 EventTracker Management Tool message box



7 Click **OK**.

EventTracker displays the result in the Notepad.

Querying Agent Service status - Group

This option enables you to query status of the agent service in the selected Group.

To query agent service status in the selected Group

1 Select the **Group** option.

2 Select the Group from the **Group Name** drop-down list.

3 Select the **Query for Agent service status** option.

4 Click **Next >**.

EventTracker displays the Enter privileged account information dialog box.

5 Type valid username and password and then click **Execute**.

EventTracker displays the EventTracker Agent Management Tool message box.

6 Click **OK**.

EventTracker displays the result in the Notepad.

Querying Agent Service status - All

This option enables you to query the agent service status running in all the systems and the Groups.

To query agent service status in all the systems and the Groups

1 Select the **All** option.

2 Select the **Query for Agent service status** option.

3 Click **Next >**.

EventTracker displays the Enter privileged account information dialog box.

4 Type valid username and password and then click **Execute**.

EventTracker displays the EventTracker Agent Management Tool message box.

5 Click **OK**.

EventTracker displays the result in the Notepad.

Restarting Agent Service - System

This option enables you to restart the agent service in the selected system.

To restart the agent service in the selected system

1 Select the **System** option.

2 Select the system from the **System Name** drop-down list.

3 Select the **Restart Agent service** option.

4 Click **Next >**.

EventTracker displays the Enter privileged account information dialog box.

5 Type valid username and password.

6 Click **Execute**.

EventTracker displays the EventTracker Agent Management Tool message box.

7 Click **OK**.

EventTracker displays the result in the Notepad.

Restarting Agent Service - Group

This option enables you to restart the agent service in the selected Group.

To restart the agent service in the selected Group

1. Select the **Group** option.
2. Select the Group from the **Group Name** drop-down list.
3. Select the **Restart Agent service** option.
4. Click **Next >**.

   EventTracker displays the Enter privileged account information dialog box.
5. Type valid username and password.
6. Click **Execute**.

   EventTracker displays the EventTracker Agent Management Tool message box.
7. Click **OK**.

   EventTracker displays the result in the Notepad.

Restarting Agent Service - All

This option enables you to restart the agent service in all the systems and the Groups.

To restart the agent service in all the systems and the Groups

1. Select the **All** option.
2. Select the **Restart Agent service** option.
3. Click **Next >**.

   EventTracker displays the Enter privileged account information dialog box.
4. Type valid username and password.
5. Click **Execute**.

   EventTracker displays the EventTracker Agent Management Tool message box.
6. Click **OK**.

   EventTracker displays the result in the Notepad.

Querying version of the Agent Service - System

This option enables you to Query the version of the agent service in the selected system.

To query the version of the agent service in the selected system

1. Select the **System** option.
2. Select the system from the **System Name** drop-down list.
3. Select the **Query for Agent version** option.
4. Click **Next >**.

   EventTracker displays the Enter privileged account information dialog box.
5. Enter valid username and password.
6. Click **Execute**.

   EventTracker displays the EventTracker Agent Management Tool message box.
7. Click **OK**.

   EventTracker displays the result in the Notepad.

Querying version of the Agent Service - Group

This option enables you to Query the version of the agent service in the selected Group.

To query the version of the agent service in the selected Group

1. Select the **Group** option.
2. Select the Group from the **Group Name** drop-down list.
3. Select the **Query for Agent version** option.
4. Click **Next >**.

   EventTracker displays the Enter privileged account information dialog box.
5. Type valid username and password.
6. Click **Execute**.

   EventTracker displays the EventTracker Agent Management Tool message box.
7. Click **OK**.

   EventTracker displays the result in the Notepad.

Querying version of the Agent Service - All

This option enables you to Query the version of the agent service in all the systems and Groups.

To query the version of the agent service in all the systems and Groups

1. Select the **All** option.
2. Select the **Query for Agent version** option.
3. Click **Next >**.

   EventTracker displays the Enter privileged account information dialog box.
4. Type valid username and password.
5. Click **Execute**.

   EventTracker displays the EventTracker Agent Management Tool message box.
6. Click **OK**.

   EventTracker displays the result in the Notepad.
7. Click **Close** to close the EventTracker Agent Management Tool.

Deploying Windows Agents in Command line mode

The advantages of Agent deployment through command line mode are as follows:

- You can specify the system name or IP address and installation path by providing appropriate command line arguments to the Agent Manager application.
- You can create a text file, mentioning the system names or IP addresses where you want to install or uninstall the Agents. This multiple Agent installation and uninstallation will be performed in silent mode i.e. without displaying any user interface.

The Agent Installer runs on the EventTracker Console and requires Domain Admin privileges. It can only be used to deploy EventTracker Agents to monitor Windows machines within the same or trusted domain.

Command line parameters

The Agent Manager application has the following command line parameters:

AgentInstaller.exe –I/-U –N:<Sys Name or IP Addr> / -F<filename> [-P:<Install path>]

Table 54

Parameter	Description
-I	To Install Agent.
-U	To Uninstall Agent.
-N	Name of the system or IP address of the system
-F	Filename supplied in place of <filename> containing the System list
-P	Installation Path for the Agent.

Examples:

1. To install an Agent in system 'SYS1' in C:\Program Files\EventTracker directory, use the following command.

AgentInstaller.exe –I –N:SYS1 –P:C:\Program Files\EventTracker

2. To uninstall an Agent from system 'SYS1', use the following command.

AgentInstaller.exe –U –N:SYS1

3. To install Agent in multiple systems, create a file "systems.txt" with system names or IP addresses and use the following command.

AgentInstaller.exe –I –F:systems.txt –P:C:\Program files\EventTracker

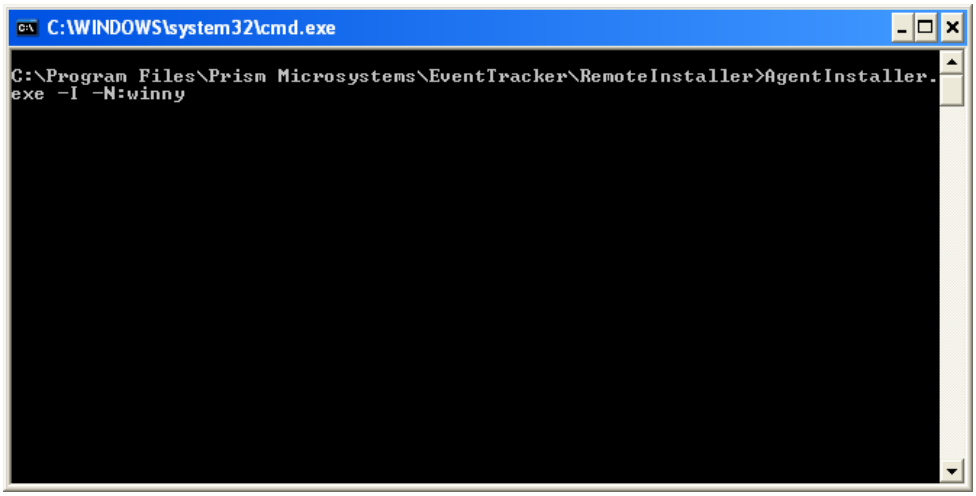
Installing Agent on a single system

This option helps you install EventTracker Agent on a single system by specifying the system name or IP address.

To install Agent in a single system

1. Open the command prompt.
2. Type the path of the **AgentInstaller.exe**. (ex: c:\program files\prism Microsystems\EventTracker\RemoteInstaller)
3. Type **AgentInstaller.exe** in the command prompt.
4. Type the switch **–I**.
5. Type the switch **–N:** followed by the name or IP address of the system where you want to install the Agent.

Figure 289 Agent installation – Command line mode



6 Press **Enter** on your keyboard.

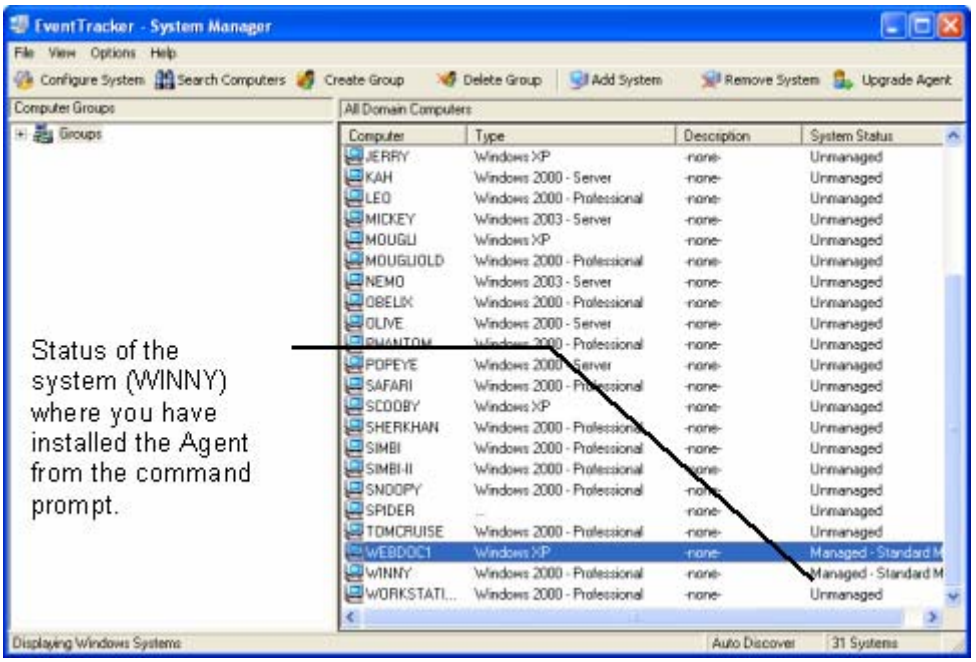
RemoteInstaller installs the Agent on the target computer.

7 Open the System Manager.

8 Press **F5** on your keyboard to refresh the console.

System Manager displays the System Status of the computer where you have installed the Agent.

Figure 290 System Manager console



Uninstalling Agent from a single system

To uninstall Agent from a system

1. Type the path of the AgentInstaller.
2. Type **AgentInstaller.exe** in the command prompt.
3. Type the switch **–U**.
4. Type the switch **–N:** followed by the name or IP address of the system from where you want to uninstall the Agent.
5. Press **Enter** on your keyboard.

   RemoteInstaller uninstalls the Agent on the target computer.

Installing and Uninstalling Agents in multiple systems

This option helps you to install EventTracker Agent in multiple systems by specifying the system names or IP addresses in a text file.

To install Agents on multiple systems

1. Create a text file and save it as **Systems.txt** in the default AgentInstaller folder.
2. Type the names or IP addresses of the systems where you want to install the Agent and save the file.
3. Open the command prompt.
4. Type the path of the **AgentInstaller.exe**.
5. Type **AgentInstaller.exe** in the command prompt.
6. Type the switch **–I**.
7. Type the switch **–F:** followed by the name of the text file (**Systems.txt**).
8. Press **Enter** on your keyboard.
9. Open the System Manager.
10. Press **F5** on your keyboard to refresh the console.

To uninstall Agents from multiple systems

To uninstall Agent from multiple system

1. Type the **–U**.

2 Type the switch **–F:** followed by the file name (**Systems.txt**) and press **Enter**.

3 Open the Agent Management Tool console and check for the Agent status.

Chapter 9
Agentless Monitoring of Windows Systems

In this chapter, you will learn how to:

- Monitor remote Windows systems without deploying Agents

Agentless Monitoring

In cases where it is not possible or desirable to install the EventTracker Windows Agent, EventTracker can be configured to periodically poll the target computers over the network to collect new event log entries since the last poll.

Pros

- No agent to deploy – Simpler product deployment. There is lesser effort during planning, deployment and upgrade.

Cons

- Increased network load – Depending on the selected polling cycle and level of event generation, network load is greater.
- Greater dependency, more critical points of failure – The Console becomes critical since it is polling target machines. Network choke points can impact performance.
- Real-time notification not possible – The earliest notifications can be sent depends on where the Console is in its polling cycle.
- Limited to operation within a domain – The Console and target machine must be in the same domain so that domain privileges are preserved.
- Performance monitoring – this feature is not available.
- Application monitoring – this feature is not available.
- Software install/removal monitoring – this feature is not available.
- Service monitoring – this feature is not available.
- Monitoring external log files – this feature is not available.
- Host based intrusion detection – this feature is not available.
- Non-domain topologies not supported – this feature is only available when the Console and target machine are in the same Windows domain.

Adding Systems for Agent-less monitoring

This option enables you to add systems from where you want to collect events periodically. The resource (CPU/memory/disk) usage, log file monitoring, and other agent required features are disabled, in the agent-less monitoring systems. Additionally, the service account of the local agent should have administrative privileges on all the systems that are added for collecting events.

To add systems for Agent-less monitoring

1. Open the System Manager.
2. Click the **Options** menu and select the **Add System** option

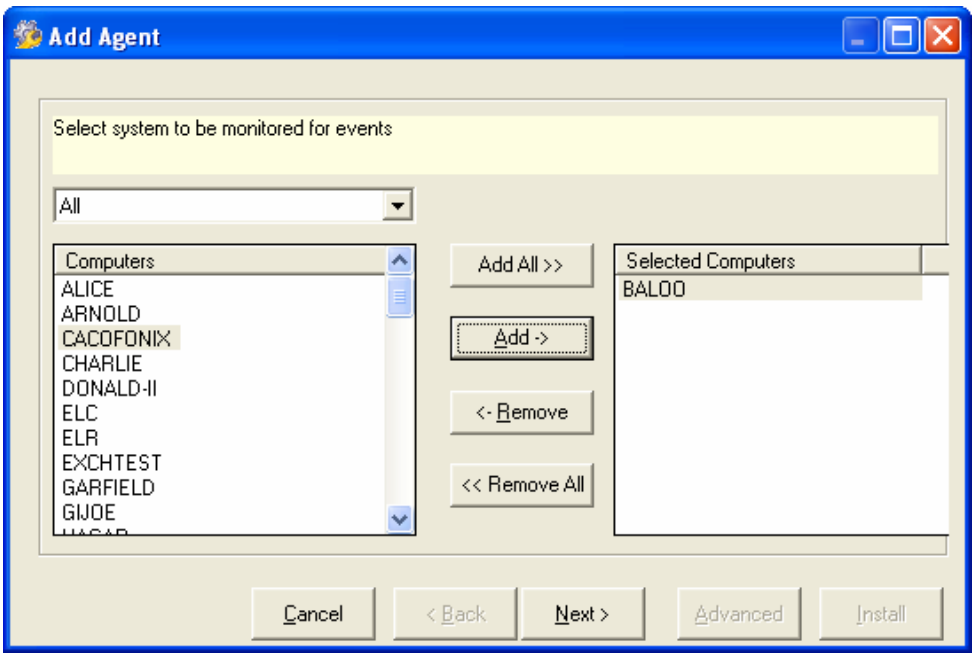
   (OR)

   Click **Add System** on the toolbar.

   System Manager displays the Add Agent window.
3. Select the computers.
4. Click **Next>**.

   System Manager displays the Add Agent window.

Figure 291 Add System window – Computer selection



5. Click **Next>**.

   System Manager displays the Add Agent window.

Figure 292 Add System window – Agent Type selection

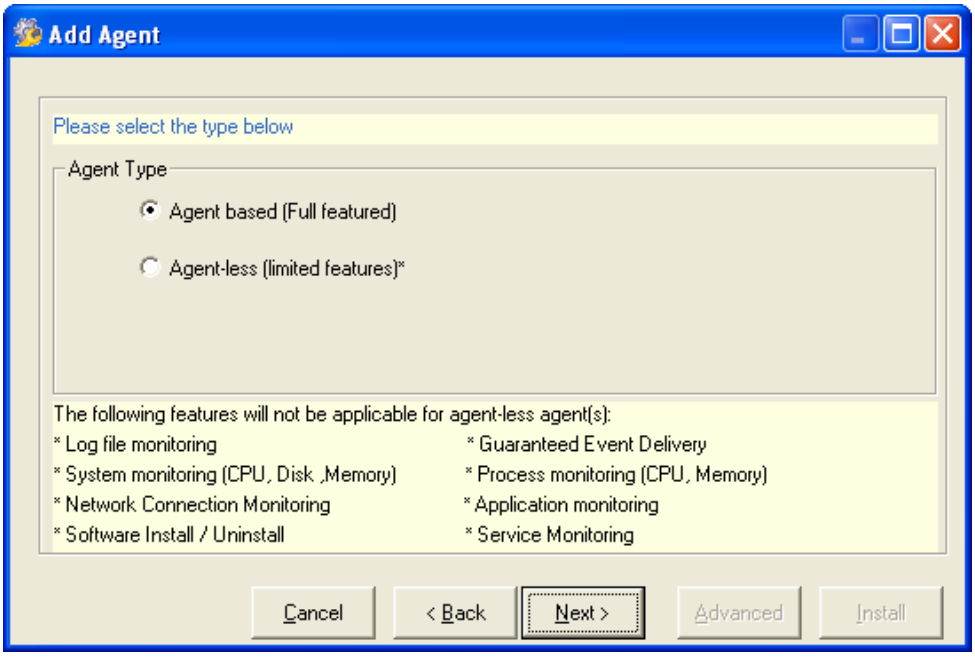


Table 55

Field	Description
Agent Type	
Agent based (Full featured)	This option enables you to install an agent in the remote system in the Standard mode. For more information, refer Installing Agents – Standard mode on page 182.
Agent-less (limited features)	Select this option to add the system with limited EventTracker Agent features. In the Agent-less type, the following features not available: ■ Log file Monitoring ■ System Monitoring ■ Network Connection Monitoring ■ Software Install / Uninstall ■ Guaranteed Event Delivery ■ Process Monitoring ■ Application Monitoring ■ Service Monitoring

6 Select the **Agent-less (limited features)*** option.

Figure 293 Add System window – Agent Type selection

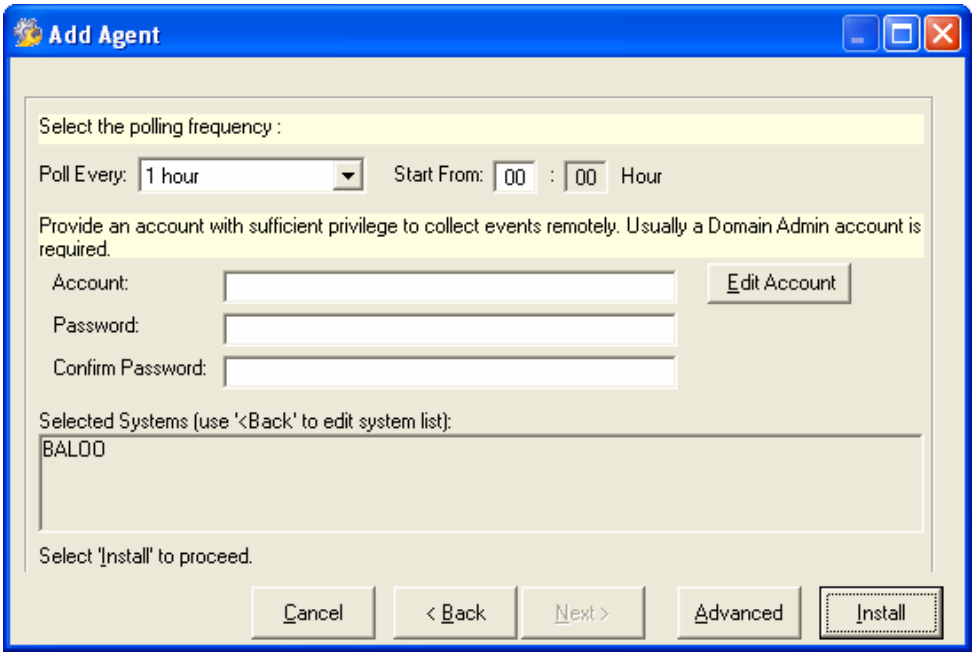


Table 56

Field	Description
Polling frequency	
Poll Every	Select the time frequency for which you want to get the events from the system, from the drop-down list.
Start From	Type the starting time from when you want to get the events from the system. This field supports `HH:MM` format.
Domain Admin account	Type valid user name and password in Account, Password and Confirm Password fields respectively.
Edit Account	Click this button to modify the admin account details.
Selected Systems	This field displays the selected system list.

7 Type appropriately in the relevant fields.

Note

To set a more specific configuration, click **Advanced** (OR) click **Install** to track the system(s).

8 Click **Advanced**.

Figure 294 Add System window – Apply configuration

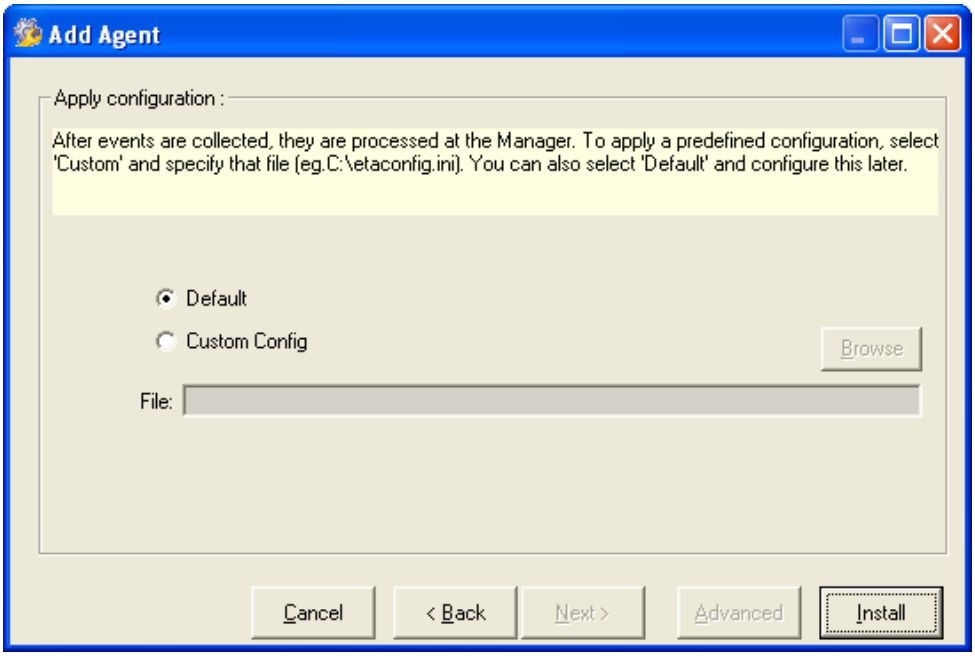
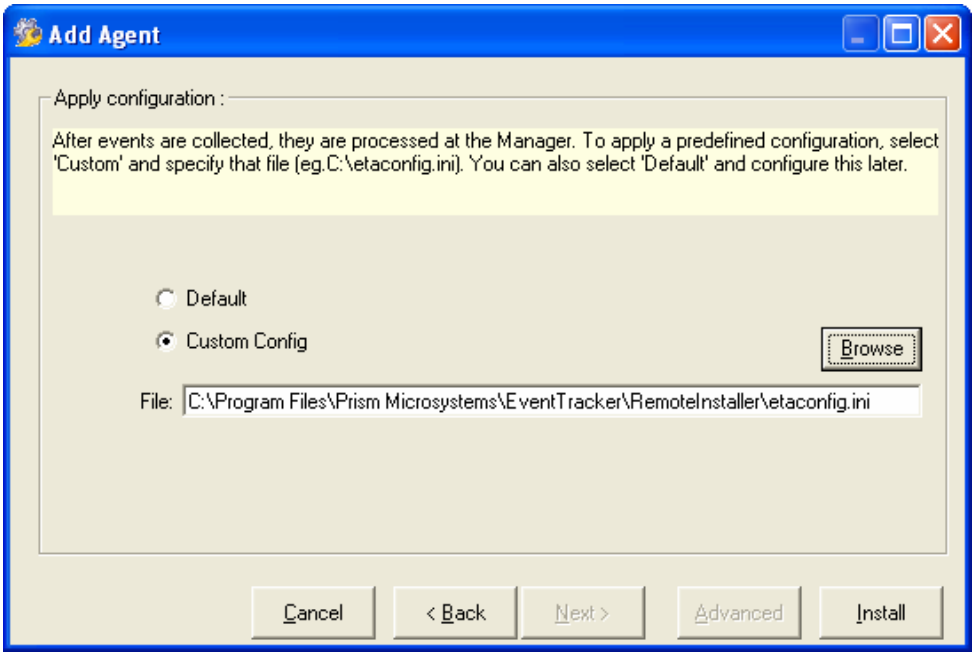

Add Agent
Apply configuration :
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify that file (eg.C:\etaconfig.ini). You can also select 'Default' and configure this later.
Default
Custom Config
Browse
File:
Cancel
< Back
Next >
Advanced
Install

Table 57

Field	Description
Default	Select this option to set the default system configuration. The default configuration will track all events.
Custom Config	Select this option to apply a different configuration. The File field is enabled. Click **Browse** and select the file. The file extension should be `.ini` format.

9 Click the appropriate system configuration.

Figure 295 Add System window – Apply configuration

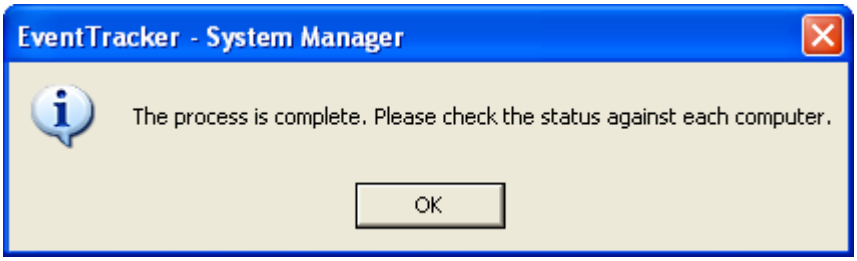

Add Agent
Apply configuration :
After events are collected, they are processed at the Manager. To apply a predefined configuration, select 'Custom' and specify that file (eg.C:\etaconfig.ini). You can also select 'Default' and configure this later.
Default
Custom Config
Browse
File:
C:\Program Files\Prism Microsystems\EventTracker\RemoteInstaller\etaconfig.ini
Cancel
< Back
Next >
Advanced
Install

10 Click **Install**.

System Manager starts adding the system and displays the progress bar.

After adding the system, System Manager displays the EventTracker – System Manager message box.

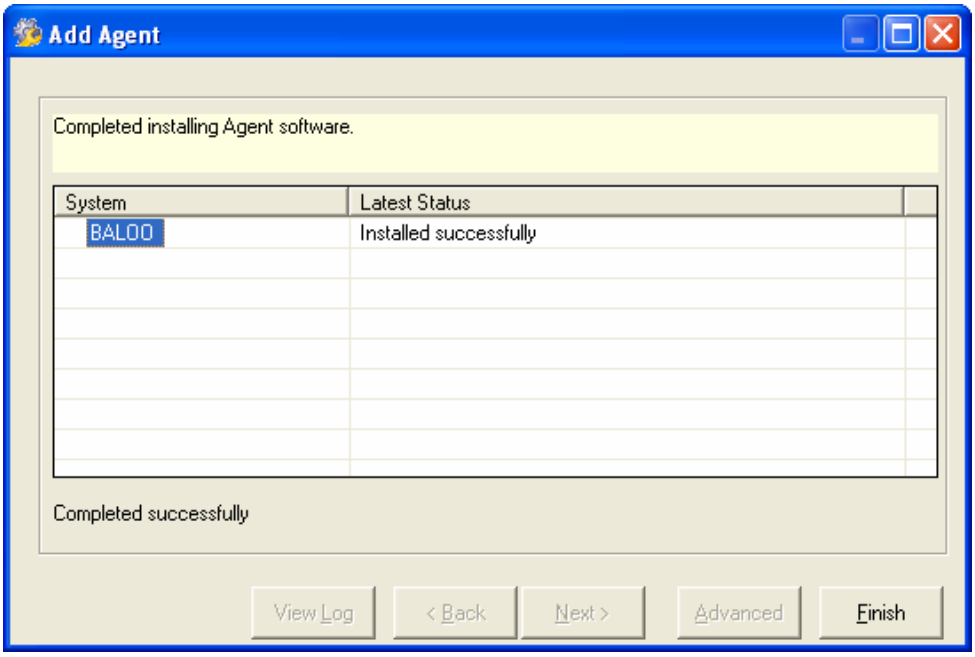
Figure 296 System Manager– message box



11 Click **OK**.

System Manager displays the successful installation message.

Figure 297 Add System window – Successful installation message



12 Click **Finish**.

Editing Admin account

This option helps you modify the admin account details. You cannot modify these details for individual systems. Once it is set, it is applicable for all the systems.

To modify admin account details

1 Add a system.

System Manager disables Account, Password and Confirm Password fields.

2 Click **Edit Account**.

System Manager displays the warning message box.

Figure 298 Change account details – warning message

EventTracker - System Manager
This account will be used to access all systems which are configured for agentless monitoring. Please ensure that you configure an account that can access these systems as an administrator.
OK

3 Click **OK** and make necessary changes.

Chapter 10
EventVault Warehouse Manager

In this chapter, you will learn how to:

- Configure EventTracker Scheduler Service account settings
- Configure EventVault Warehouse Manager
- Backup EventVault Data
- Save EventBox Information
- Verify EventBox Integrity
- Extract EventBox Data
- Delete EventBox
- Append CAB files
- View CAB files for a specific period
- Move Archives to a new location

EventTracker stores all received events in EventVault, an optimized and high performance event warehouse that is purpose-built for efficient storage and retrieval of event logs. EventVault reliably and efficiently archives event logs from across the enterprise without the need for any DBMS licenses or the overhead of Database Administrators. All collected events are compressed (over 90% compression ratio), encrypted and sealed with a SHA-1 signature to prevent potential tampering.

EventTracker Scheduler service

The functionality of legacy EventTracker Scheduler service has been enhanced to align with Collection Point architecture. The functionality varies with respect to the Console type you select while installing EventTracker v5.6.

If you select Standard Console, then the functionality of EventTracker Scheduler service remains unaltered as in earlier versions of EventTracker.

If you select Collection Master or Collection Point Console, then the functionality varies accordingly.

EventTracker Scheduler service monitors and manages Log Volume Analyzer schedules and EventVault Integrity check schedules. EventTracker logs the service related information in etslog.txt file, which is available in the default EventTracker installation folder typically …\Program Files\Prism Microsystems\EventTracker. EventTracker logs Log Volume Analyzer schedule related information in etrptschlog.txt, which is available in …\Program Files\Prism Microsystems\EventTracker folder and EventVault integrity check related information in CABIntChkLog.txt, which is available in …\Program Files\Prism Microsystems\EventTracker\Archives folder.

If the …\Program Files\Prism Microsystems\EventTracker\Archives folder is on a remote machine across the network, crosscheck the following:

EventTracker Scheduler service account settings: Check if the EventTracker Scheduler service account has Administrator privilege on the remote machine. If the EventTracker Scheduler service does not have the mandatory privilege do the following:

1. Open Services.msc
2. Right-click EventTracker Scheduler.
3. From the shortcut menu, choose the Properties option.
4. Click the Log On tab.
5. Select the This account option.
6. Type valid user name and password, which has Administrator privilege on the remote machine where the CAB files reside.
7. Click Apply.

Firewall settings (Example: Windows Firewall): When the EventTracker Scheduler service tries to access CAB files on the remote machine, the Firewall may deny access to the remote machine. Allow Firewall to permit EventTracker Scheduler service to access CAB files on the remote machine.

Collection Master and Collection Point communicate through port **14507**.

You can also add EventTracker Scheduler service to Exceptions Programs and Services list in Windows Firewall by doing the following:

1. Open Windows Firewall settings window.
2. Click the Exceptions tab.

3 Click Add Program…
4 Click Browse and add the EventTracker Scheduler service to Programs and Services list.

EventTracker Scheduler service – Collection Master Console

EventTracker Scheduler service at Collection Master Console behaves as a server and will always be in "Listen" mode. Any number of Collection Points could be connected to Collection Master.

EventTracker Scheduler service – Collection Point Console

EventTracker Scheduler service at Collection Point Console wakes up once in 30 seconds and launches CollectionPointConfig.exe. This exe in turn will query the issdbv3 database for new CAB files to be sent to the Collection Master.

Viewing CAB files

This option helps you view CAB files for a specific period.

To view CAB files

1 Double-click **EventVault Warehouse Manager** on the Control Panel.

(OR)

Click Start, point to Programs, point to Prism Microsystems, point to EventTracker, and then select **EventVault Warehouse Manager** option.

EventTracker displays the EventVault Warehouse Manager.

By default, EventVault Warehouse Manager selects the **Show All** option and displays all the CAB files.

2 Select the **Show older than** option to view CAB files older than a specific period.

3 Select the date from the calendar controls and time from the spin box.

4 Click **Show**.

EventVault Warehouse Manager displays the CAB files older than the specified period.

5 Select the **Show From** option to view CAB files for a specific period.

6 Select the date from the calendar controls and time from the spin boxes.

7 Click **Show**.

EventVault Warehouse Manager displays the CAB files for the specified period.

Configuring EventVault

This option enables you to configure the **EventVault Warehouse Manager** to archive the events from EventTracker database. By default, EventTracker operates in High Performance mode. In this mode, EventBoxes are created automatically based on two criteria, 1. When the Cache db reaches 50 MB or 2. EventVault Schedule frequency set by selecting the number of days from the **Frequency** drop-down list in the EventVault Warehouse Manager **Configuration** dialog box.

To configure EventVault

1 Open the EventVault Warehouse Manager.

2 Click the **Options** menu and select the **Configuration** option

(OR)

Click **Configuration** on the toolbar.

EventVault Warehouse Manager displays the Configuration window.

Figure 299
Configuration dialog box

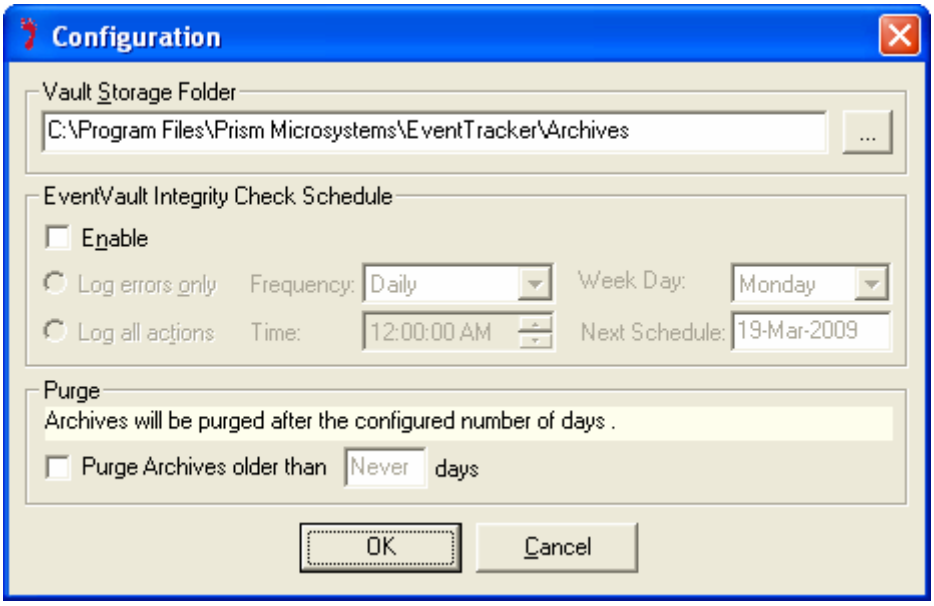


Table 58

Field	Description
Vault Storage Folder	Type or browse the path of the folder where you want to archive the event data.

Field	Description
EventVault Integrity Check Schedule	
Enable	Select this check box to schedule EventVault Integrity check. When you select this check box, EventVault Warehouse Manager will enable Log errors only and Log all actions options. EventVault Integrity check schedule and Event Traffic Analysis schedule are taken care by EventTracker Scheduler service. EventTracker logs two events, 2020 and 2021 for the start and end of Integrity check processes respectively in the Windows Application log.
Frequency	Select the frequency from this drop-down list. The available options are Daily, Twice Daily and Weekly.
Log errors only	Select this option to log only error events.
Log all actions	Select this option for logging both success and failed Integrity check and Extraction of CAB files. EventTracker logs four events, 2016 for failed Integrity check, 2017 for successful Integrity check, 2018 for failed EventBox Extraction and 2014 for successful EventBox Extraction. If this check box is not selected EventTracker logs two events 2016 and 2018.
Time	Select the time from this spin box.
Week Day	This drop-down list is enabled when you select the Frequency as Weekly. This option facilitates on which day of the week you want to start the integrity check.
Next Schedule	Displays the date of schedule. Date depends on the time you enter or select from the Time spin box. The following examples will give you a clear idea. Example 1: Current system date: 26th Feb 09 Current system time: 11:00 A.M. Frequency: Daily If you enter or select past time from the current system time from the Time spin box, EventVault Warehouse Manager will schedule the integrity check for the following day i.e. 27th Feb 09. If you enter or select future time from the current system time from the Time spin box, EventVault Warehouse Manager will schedule the integrity check on the same day i.e. 26th Feb 09. Example 2: Current system date: 26th Feb 09 Current system time: 11:00 A.M. Frequency: Twice Daily If you enter or select past time from the current system time from

Field	Description
	the Time spin box, say for instance 10:30 A.M., EventVault Warehouse Manager will schedule the first integrity check on the same day i.e. 26th Feb 09 10:30 P.M & the second integrity check will be done on the following day i.e. 27th Feb 09 10:30 A.M. If you enter or select future time from the current system time from the Time spin box, say for instance 11:30 A.M., EventVault Warehouse Manager will schedule the first integrity check on the same day i.e. 26th Feb 09 11:30 A.M & the second integrity check will be done on the same day i.e. 26th Feb 09 11:30 P.M. Example 3: Current system date: 26th Feb 09 Current system time: 11:00 A.M. Frequency: Weekly Day: Friday If you enter or select past time from the current system time from the Time spin box, say for instance 10:30 A.M., EventVault Warehouse Manager will schedule the integrity check for the following week i.e. 5th Mar 09 10:30 A.M. If you enter or select future time from the current system time from the Time spin box, say for instance 11:30 A.M., EventVault Warehouse Manager will schedule the integrity check for the following week i.e. 5th Mar 09 11:30 A.M.
Purge Archives older than	Select this check box and enter the number of days to retain CAB files. CAB files will be purged after the specified number of days. By default, EventVault Warehouse Manager retains CAB files forever.

3 Type/select appropriately in the relevant fields.

4 Click **OK**.

Note

EventTracker saves the archive files in the selected location with `.cab` extension.

Backing up EventVault Data

This option enables you to backup EventVault data locally or remotely in a desired location for a long-term storage. It helps you to retrieve the backup data if the archives are tampered.

To backup EventVault data

1. Open the EventVault Warehouse Manager.
2. Select the CAB file(s) from the **Available EventBoxes** list.

   (OR)

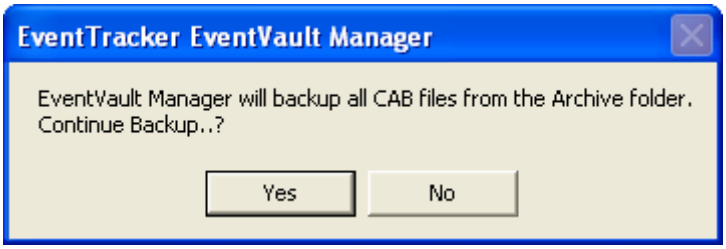
   Select the **Select All** check box to select all the archive files.
3. Click the **File** menu and select the **Backup EventVault** option

   (OR)

   Click **Backup Archives** on the toolbar.

   EventVault Warehouse Manager displays EventTracker EventVault Manager message box.

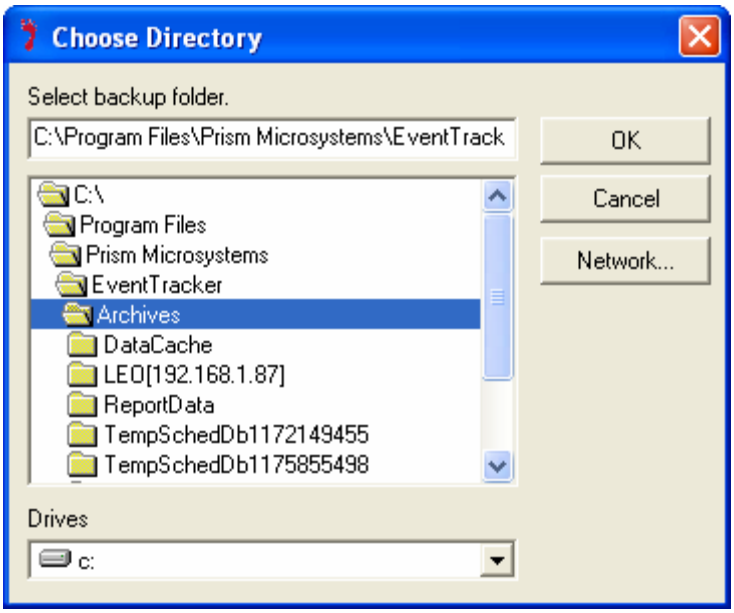
Figure 300 EventTracker EventVault Manager message box



4. Click **Yes**.

   EventVault Warehouse Manager displays the Choose Directory window.

Figure 301 Choose Directory dialog box



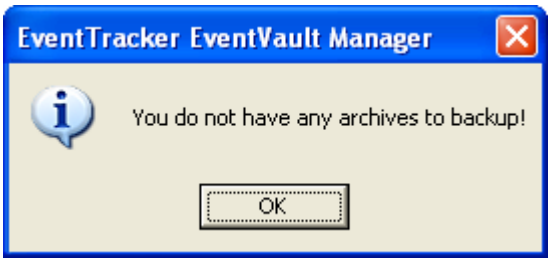
5. Select the folder where you want to store the event data.

6 Click **OK**.

EventVault Warehouse Manager displays the **ArchIntegrity** report in the Notepad after successful completion of backup.

If there is no archive file to back up, EventVault Warehouse Manager displays the EventTracker EventVault Manager message box.

Figure 302 Backup data – message box



Saving EventBox Metadata

This option enables you to save the archive summary in a text file. It helps you to locate particular `.cab` files to view, retrieve or extract events.

To save EventBox information

1 Open the EventVault Warehouse Manager.

2 Select the CAB file(s) from the **Available EventBoxes** list.

(OR)

Select the **Select All** check box to select all the archive files.

3 Click the **File** menu and select the **Save EventBox Metadata** option

(OR)

Click **Save EventBox Metadata** on the toolbar.

EventVault Warehouse Manager displays the Save As window.

EventVault Warehouse Manager saves the EventBox Info in archive-info.txt file. You can also type the file name in the **File name** field.

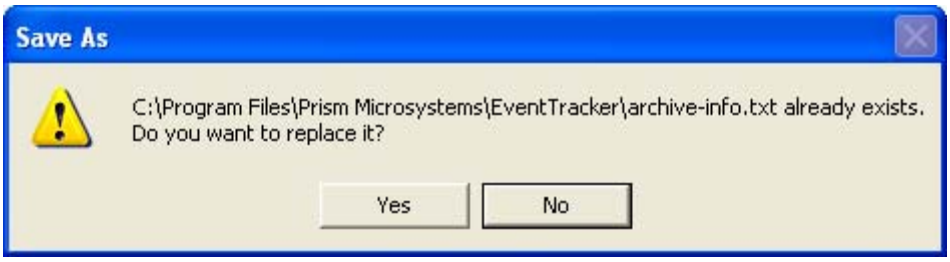
4 Select the path where you want to store the archive summary.

5 Click **Save**.

6 Open the **archive-info** text file. The contents are displayed.

EventVault Warehouse Manager displays the Save As message box, if the file already exists.

Figure 303 Save As – message box



Verifying EventBox Integrity

This option enables you to verify contents of the EventBox are intact. This will calculate a SHA1 hash value on the EventBox contents and compare with the original value. If the integrity check fails, re-index the archive database using Archive Indexer utility available under Maintenance Tools.

While verifying the integrity of an EventBox, EventVault Warehouse Manager performs the following actions

- The SHA1 checksum of the selected archive is regenerated.
- This new checksum is compared with the older (existing in the database) checksum.
- If the two checksums do not match then an error message is displayed indicating that the data has been tampered.
- If the two checksums match then it means that the data is intact.

To verify EventBox integrity

1. Open the EventVault Warehouse Manager.
2. Select the CAB files from the **Available EventBoxes** list.

   (OR)

   Select the **Select All** check box to select all the EventBoxes.
3. Click the **Options** menu and select the **Verify EventBox** option

   (OR)

   Click **Verify,** located at the bottom of the console.

   After verifying the integrity, EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad.

Extracting EventBox Data

This option enables you to extract the EventBox data into an MS Access database.

To extract EventBox data

1. Open the EventVault Warehouse Manager.
2. Select the CAB files from the **Available EventBoxes** list.

   (OR)

   Select the **Select All** check box to select all the EventBoxes.
3. Click the **Options** menu and select the **Extract EventBox** option

   (OR)

   Click **Extract,** located at the bottom of the console.

   EventVault Warehouse Manager displays the Choose Directory dialog box.
4. Select the path where you want to store the event data.
5. Click **OK**.

   After extracting the event data, EventTracker displays the ArchIntegrity report in the Notepad.

Note

EventVault Warehouse Manager saves the extracted `.cab` file in the selected location with `.mdb` file extension. You can view the database file using MS Access.

Deleting an EventBox

This option enables you to delete an existing EventBox.

To delete an EventBox

1. Open the EventVault Warehouse Manager.
2. Select the CAB files from the **Available EventBoxes** list.

   (OR)

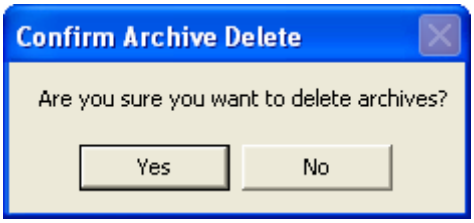
   Select the **Select All** check box to select all the EventBoxes.
3. Click the **File** menu and select the **Delete EventBox** option

(OR)

Click **Delete,** located at the bottom of the console.

EventVault Warehouse Manager displays the Confirm Archive Delete confirmation message box.

Figure 304 Delete EventBox – confirmatory message box



4 Click **Yes**.

The selected EventBox is deleted from the **Available EventBoxes** list.

After deleting the EventBox, EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad.

Moving CAB files

This option helps you move all or selected CAB files to a new location. After physically moving the CAB files, EventTracker updates the index file (etwarindex.mdb). Moving the CAB files to a new location does not harm your scheduled reports. You can run on demand reports, define reports and even configure new scheduled reports as you normally do.

To move CAB files

1 Open the EventVault Warehouse Manager.

2 Select the CAB files from the Available EventBoxes list.

(OR)

Select the **Select All** check box to select all the EventBoxes.

3 Click **Move**.

EventVault Warehouse Manager displays the confirmation message box.

Figure 305 Delete EventBox – confirmatory message box

4 Click **Yes** to proceed.

EventVault Warehouse Manager displays the Choose Directory dialog box.

5 Select the location (local or network) and then click **OK**.

EventVault Warehouse Manager moves all the selected files to the new location and displays the ArchIntegrity report in the Notepad.

Appending CAB Files

When you manually copy CAB files from different sources to the EventTracker archives folder, you have to recreate the archives index (etwarindex.bin) file with the help of **Archive Indexer** tool (Control Panel -> Maintenance Tools -> Archive Indexer). This is a very time consuming process if you are copying a huge volume of CAB files.

The Append Archives feature helps you to append the timeticks, name and checksum information about the new CAB files to the existing archive index file with minimal time consumption.

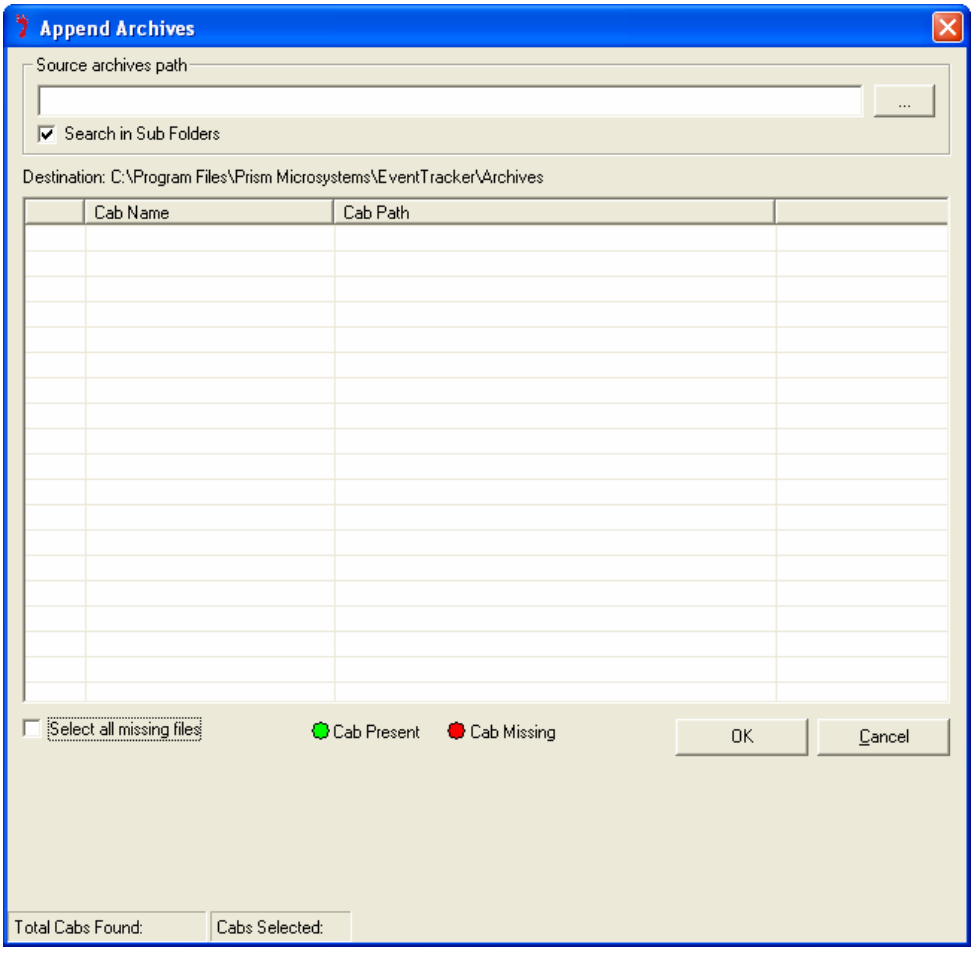
To append CAB files

1 Open the EventVault Warehouse Manager.

2 Click **Append Archives** on the toolbar.

EventVault Warehouse Manager displays the Append Archives window.

Figure 306 Append Archives window



Indicates the CAB files present in the Archives folder. EventVault Warehouse Manager will ignore redundant CAB files.

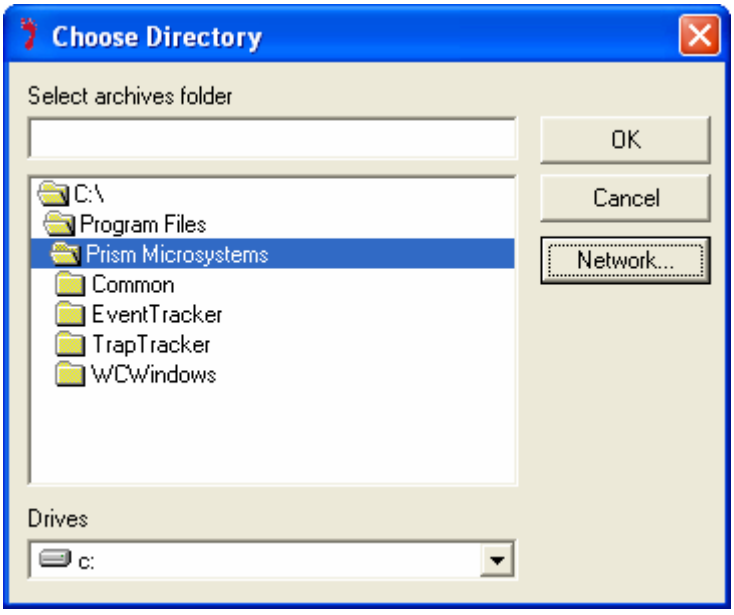
Indicates that the CAB files are not present in the destination folder i.e. EventTracker Archives folder.

After creating the index file, EventVault Warehouse Manager displays the Append Archives window with actual physical files present in the Archives folder.

Search in Sub Folders check box is selected by default. Clear this check box to append archives in the root folder alone and not in the sub folders.

3 Click ... and select the path of the folder where you have stored the CAB files.

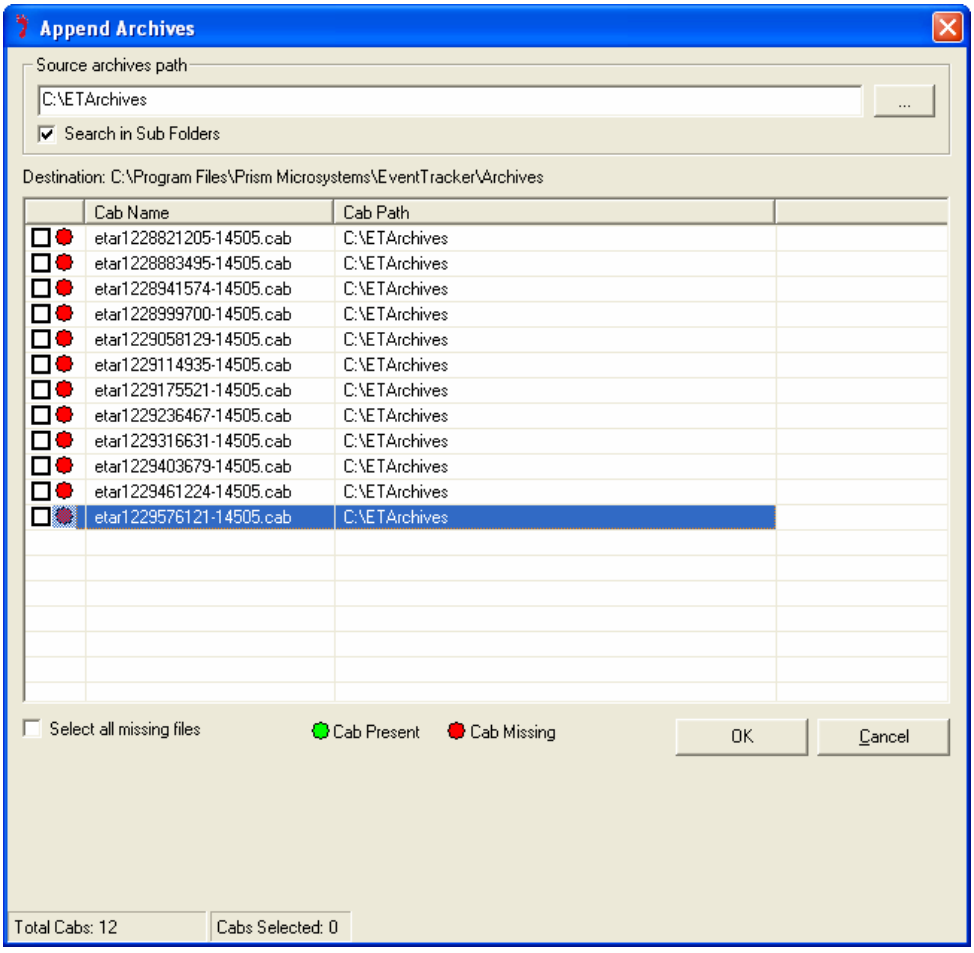
Figure 307 Choose Directory window



4 Click **OK**.

EventVault Warehouse Manager displays the Append Archives window.

Figure 308 Append Archives window

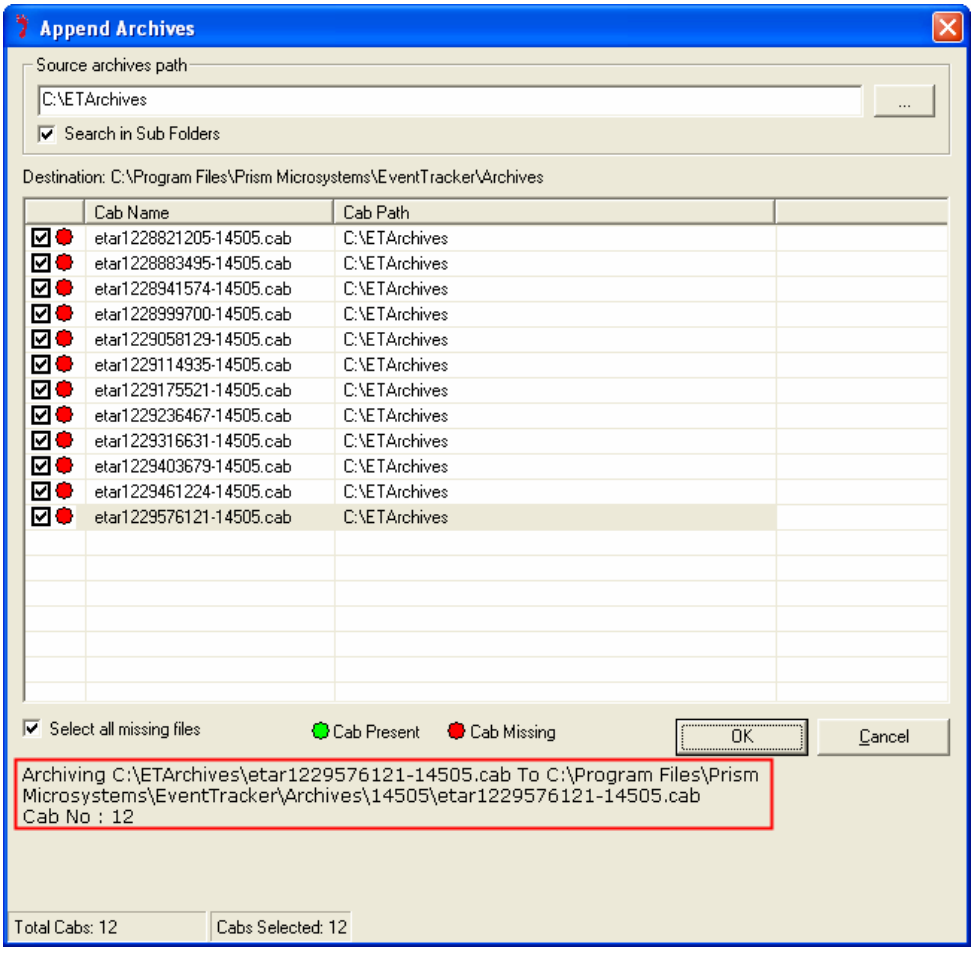


You can select individual files by selecting the check boxes against the respective CAB files or collectively by selecting the Select all missing cabs.

5 Click **OK**.

EventVault Warehouse Manager displays the progress of appending process.

Figure 309 Append Archives window



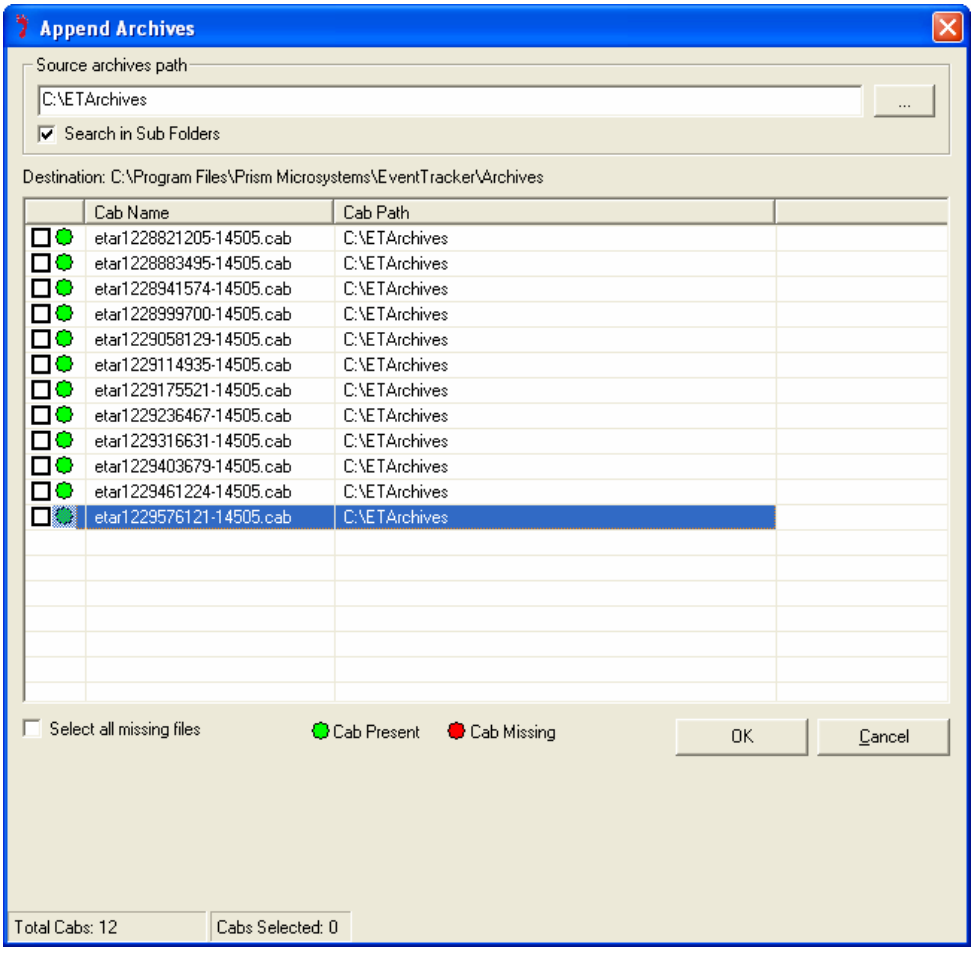
After the successful completion, EventVault Warehouse Manager displays the ArchiveAppender message box.

Figure 310 ArchiveAppender message box

6 Click **OK**.

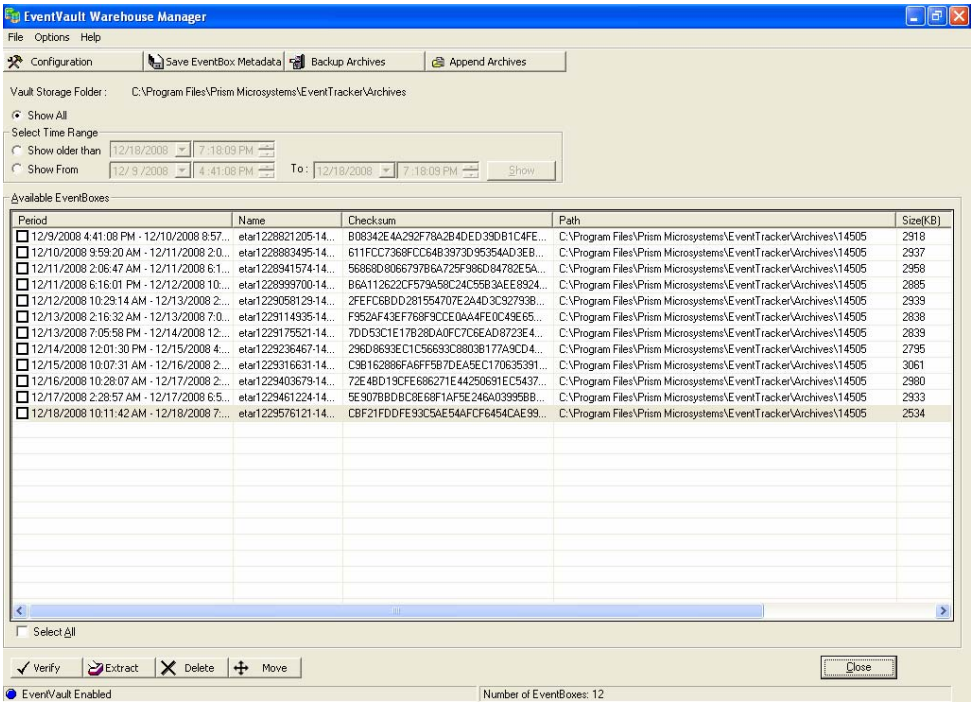
EventVault Warehouse Manager displays the Append Archives window.

Figure 311 Append Archives window



EventVault Warehouse Manager appends the cab files to the appropriate folders.

Figure 312 EventVault Warehouse Manager


EventVault Warehouse Manager
File Options Help
Configuration
Save EventBox Metadata
Backup Archives
Append Archives
Vault Storage Folder : C:\Program Files\Prism Microsystems\EventTracker\Archives
Show All
Select Time Range
Show older than 12/18/2008 7:18:09 PM
Show From 12/ 9 /2008 4:41:08 PM To : 12/18/2008 7:18:09 PM Show
Available EventBoxes
Period Name Checksum Path Size(KB)
12/9/2008 4:41:08 PM - 12/10/2008 8:57... etar122882120514... B08342E4A292F78A2B4DED39DB1C4FE... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2918
12/10/2008 9:59:20 AM - 12/11/2008 2:0... etar122888349514... 611FCC7368FCC64B3973D95354AD3EB... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2937
12/11/2008 2:06:47 AM - 12/11/2008 6:1... etar122894157414... 56868D8066797B6A725F986D84782E5A... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2958
12/11/2008 6:16:01 PM - 12/12/2008 10:... etar122899970014... B6A112622CF579A58C24C55B3AEE8924... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2885
12/12/2008 10:29:14 AM - 12/13/2008 2:... etar122905812914... 2FEFC6BDD281554707E2A4D3C92793B... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2939
12/13/2008 2:16:32 AM - 12/13/2008 7:0... etar122911493514... F952AF43EF768F9CCE0AA4FE0C49E65... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2838
12/13/2008 7:05:58 PM - 12/14/2008 12:... etar122917552114... 7DD53C1E17B28DA0FC7C6EAD8723E4... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2839
12/14/2008 12:01:30 PM - 12/15/2008 4:... etar122923646714... 296D8693EC1C56693C8803B177A9CD4... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2795
12/15/2008 10:07:31 AM - 12/16/2008 2:... etar122931663114... C9B162886FA6FF5B7DEA5EC170635391... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 3061
12/16/2008 10:28:07 AM - 12/17/2008 2:... etar122940367914... 72E4BD19CFE686271E44250691EC5437... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2980
12/17/2008 2:28:57 AM - 12/17/2008 6:5... etar122946122414... 5E907BBDBC8E68F1AF5E246A03995BB... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2933
12/18/2008 10:11:42 AM - 12/18/2008 7:... etar122957612114... CBF21FDDFE93C5AE54AFCF6454CAE99... C:\Program Files\Prism Microsystems\EventTracker\Archives\14505 2534
Select All
Verify Extract Delete Move Close
EventVault Enabled
Number of EventBoxes: 12

Chapter 11
Analysis

In this chapter, you will learn how to:

- Search Log
- Analyze Event Traffic
- Analyze User Activity
- Analyze ROI

EventTracker Log Search

Filter and display event logs based on user-defined criteria. The user can define the filter (or exclude) string as well as specify the output format.

Usage: Forensic Analysis of specific events, broad searches per criteria with subsequent sorting and ordering of the result set.

For more information refer EventTracker Log Search guide.

Event Traffic Analysis

After EventTracker is deployed on numerous systems in a large Network it is very likely that you notice EventTracker receiving millions of events. Actually a majority of these events would be of little use to you. Using appropriate priority you can filter out unnecessary events to improve utility. `Filtering unnecessary events' is a powerful feature based on priority configured by you.

Traffic Analyzer is a tool that is part of the EventTracker Console. It helps to find the details of the most common events and to set your order of priority. Accordingly create filters for non-essential events that are just increasing traffic but have little value.

Filtering is a continuous process. Priority may vary from one system to another. Over a period of time, with your experience, priority events can be separated from non-priority events in a specific system. Repeating this process every week enables you to receive only events of value in optimizing your operations. When non-priority events are filtered out EventTracker functions optimally.

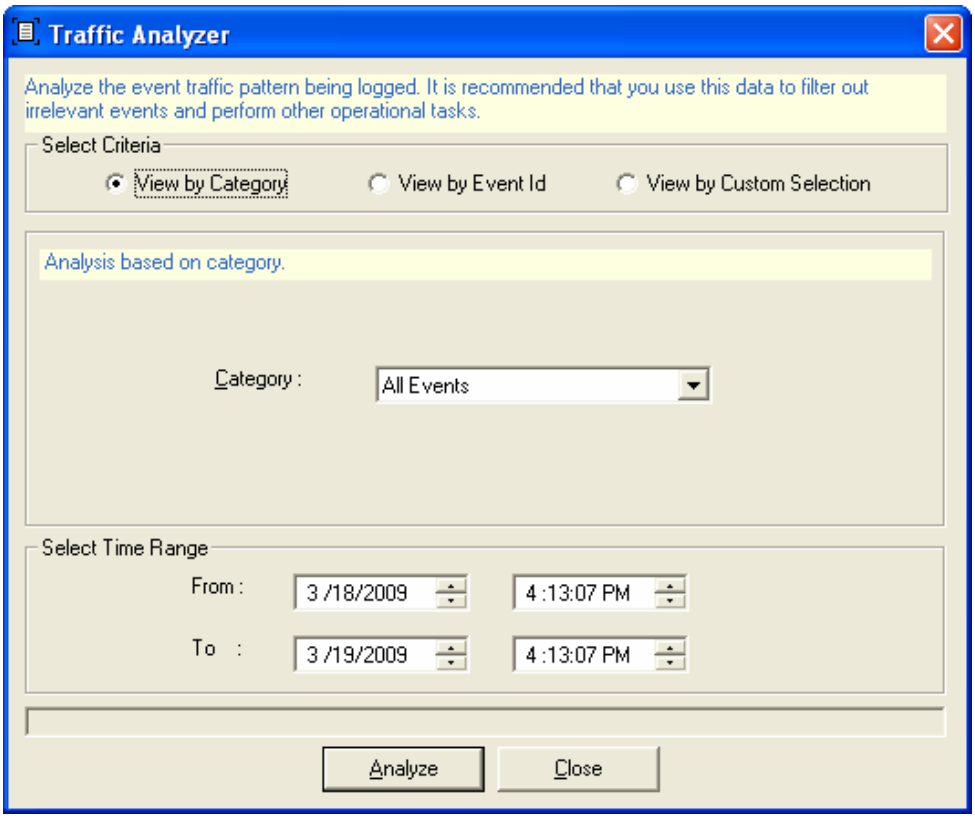
This report provides total counts per system for each event id. Filter and display event count details based on user-defined criteria.

Usage: Analyze Windows specific security events, correlate events, broad searches per criteria with subsequent sorting and ordering of the result set.

1. Open the Management Console.
2. Click the **Tools** menu and select the **Traffic Analyzer** option.

   EventTracker displays the Traffic Analyzer.

Figure 313 Traffic Analyzer



Traffic Analysis – View by Category

This option helps you analyze events based on Category.

To analyze event traffic – View by Category

1. Select the **View by Category** option.
2. Select a Category from the **Category** drop-down list. Example: All Warning Events.
3. Set the From, To date and time range through the **From**, **To** spin boxes.
4. Select the systems.
5. Click **Analyze**.

   EventTracker displays the report in the Notepad.

Correlating Events

This option enables you to correlate events with the offline events in the database.

To correlate events

1. Open the Management Console.
2. Click the **Tools** menu and select the **Traffic Analyzer** option.
3. Select the **All Correlation Events** option from the Category drop-down list.
4. Set the From, To date and time range through the **From**, **To** spin boxes.
5. Select the systems.
6. Click **Analyze**.

   EventTracker displays the analysis report EvtTrfcAnalyze in the Notepad.

Traffic Analysis – View by Event Id

This option helps you analyze hard coded Windows specific security events.

To analyze event traffic – View by Event Id

1. Open the Management Console.
2. Click the **Tools** menu and select the **Traffic Analyzer** option.
3. Select the **View by Event Id** option.

Figure 314 Traffic Analyzer

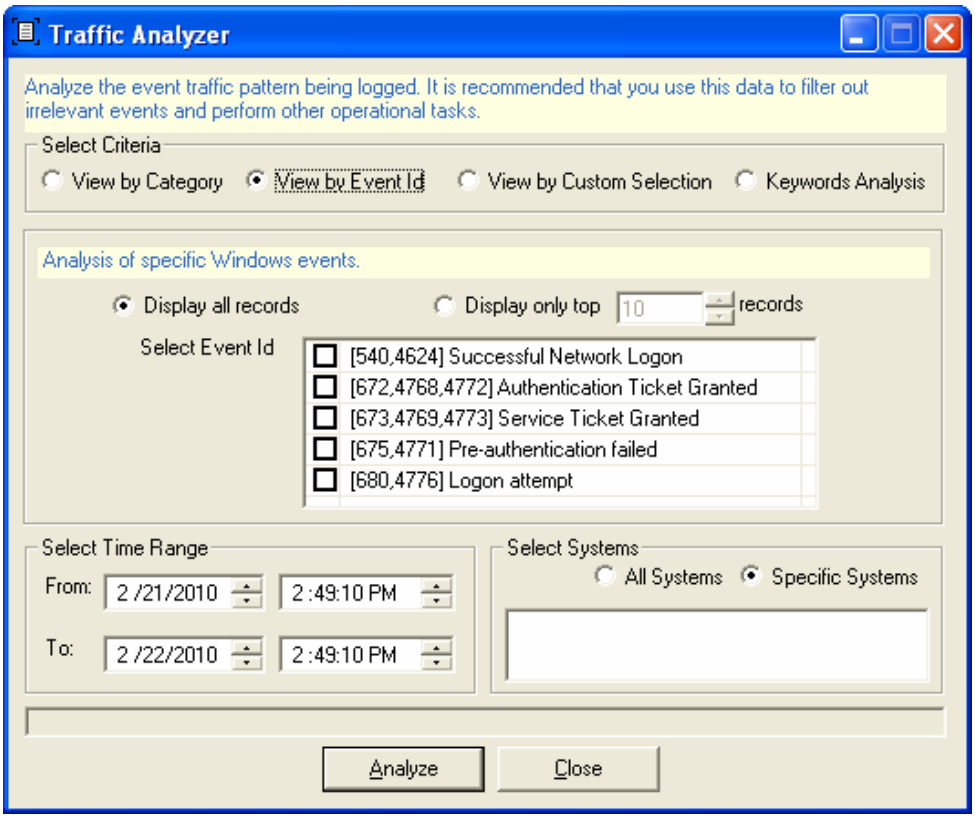


Table 59

Field	Description
Display all records: By default this option is selected. All records will be displayed in the report in descending order.	
Display only top: You can select this option if you want only a specified number of records to be displayed in the report.	
Select Event Id: You can select 5 hard coded Windows security events for event traffic analysis.	
540 Successful Network Logon	Selecting this id will generate 2 reports sorted by **Username** and **IP address**.
672 Authentication Ticket Granted	Selecting this id will generate 2 reports sorted by **Username** and **IP address**.
673 Service Ticket Granted	Selecting this id will generate 1 report sorted by **IP Address**.
675 Pre-authentication failed	Selecting this id will generate 2 reports sorted by **Username** and **IP address**.

Field	Description
Display all records: By default this option is selected. All records will be displayed in the report in descending order.	
Display only top: You can select this option if you want only a specified number of records to be displayed in the report.	
Select Event Id: You can select 5 hard coded Windows security events for event traffic analysis.	
680 Logon attempt	Selecting this id will generate 2 reports sorted by **Username** and **Computer**.

4 Type / select appropriately in the relevant fields.

5 Select the systems.

6 Click **Analyze**.

EventTracker displays the report in the Notepad.

If you wish to display only a specified number of records in the report, type the number of records in the **Display only top** field or click the spin box.

Traffic Analysis – View by Custom Selection

This option helps you customize the selection criteria.

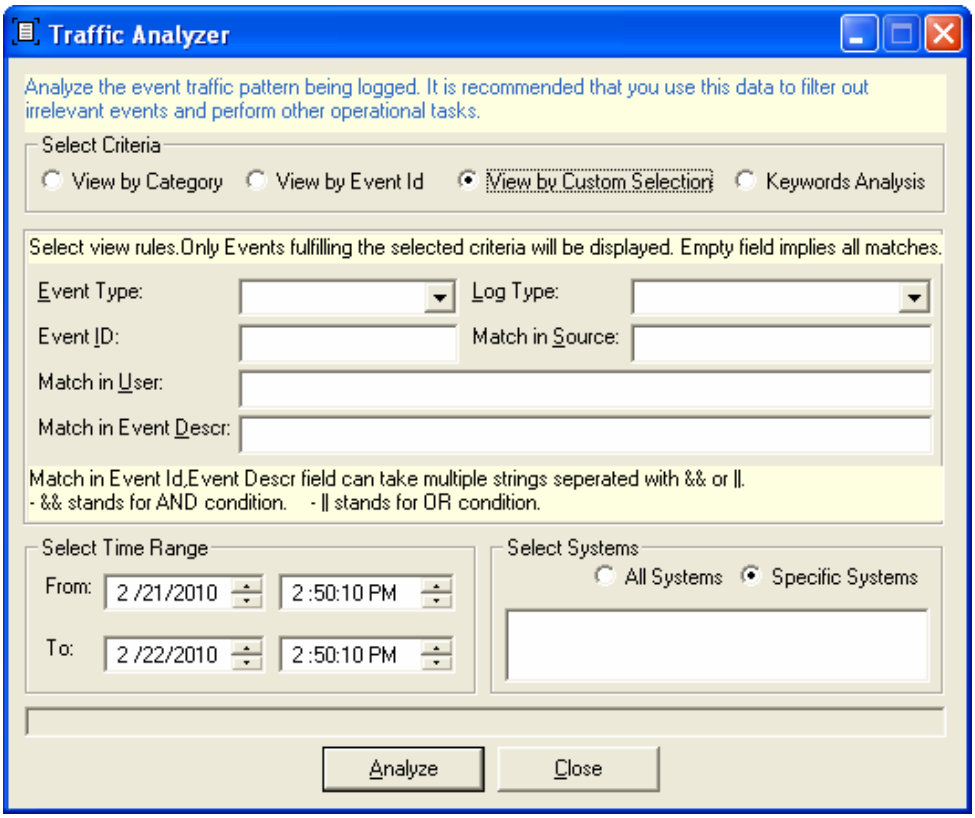
To analyze event traffic – View by Custom Selection

1 Open the Management Console.

2 Click the **Tools** menu and select the **Traffic Analyzer** option.

3 Select the **View by Custom Selection** option.

Figure 315 Traffic Analyzer


Traffic Analyzer
Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.
Select Criteria
View by Category
View by Event Id
View by Custom Selection
Keywords Analysis
Select view rules.Only Events fulfilling the selected criteria will be displayed. Empty field implies all matches.
Event Type:
Log Type:
Event ID:
Match in Source:
Match in User:
Match in Event Descr:
Match in Event Id,Event Descr field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Select Time Range
From:
2 /21/2010
2 :50:10 PM
To:
2 /22/2010
2 :50:10 PM
Select Systems
All Systems
Specific Systems
Analyze
Close

4 Type appropriately in the relevant fields.

5 Select the systems.

6 Click **Analyze**.

EventTracker displays the report in the Notepad.

Traffic Analysis – Keyword Analysis

This option helps to analyze traffic by keywords.

To analyze event traffic – by keywords

1 Open the Management Console.

2 Click the **Tools** menu and select the **Traffic Analyzer** option.

3 Select the **Keywords Analysis** option.

Figure 316 Traffic Analyzer

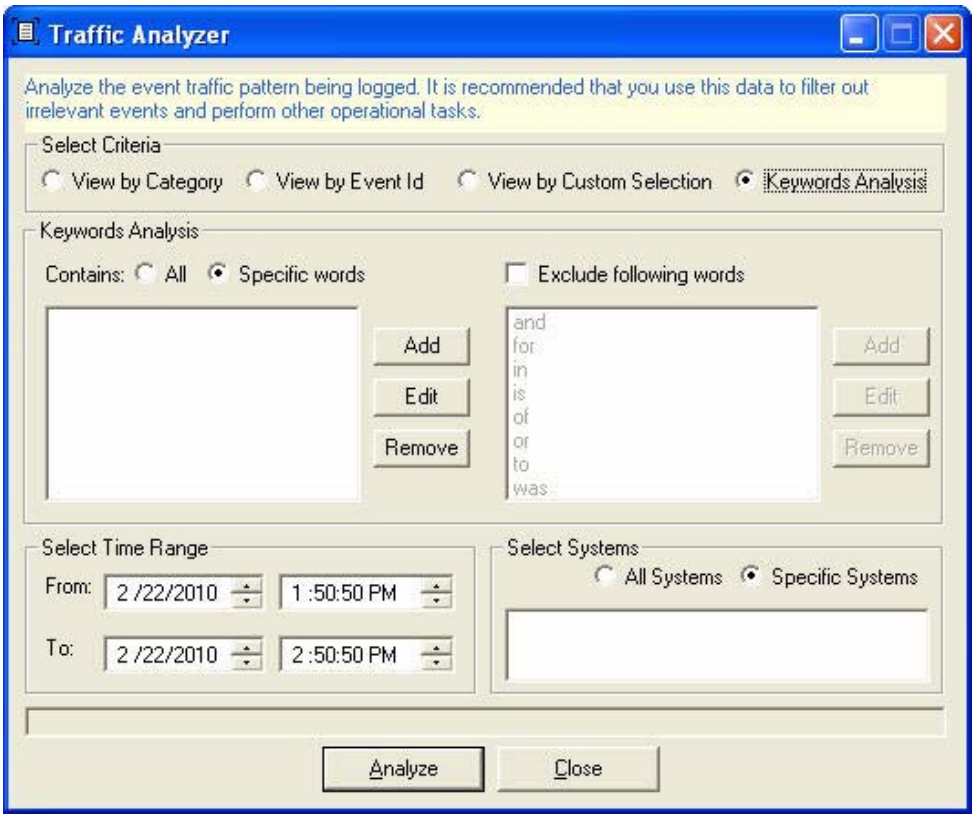
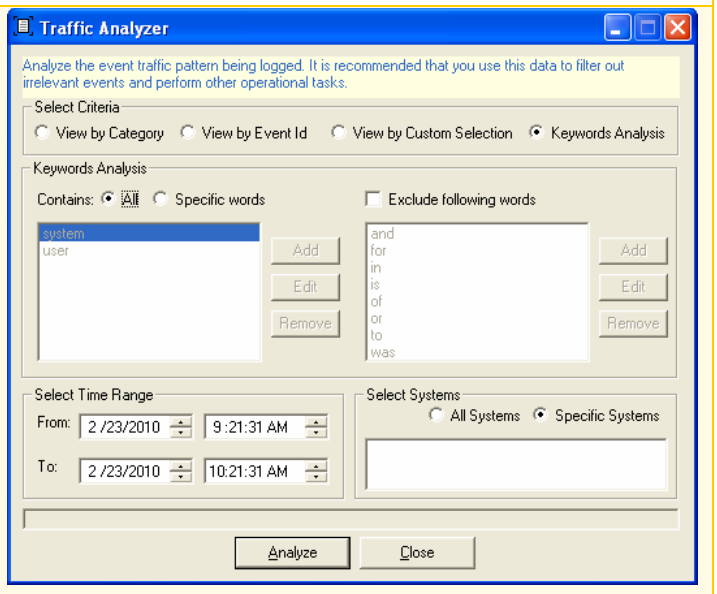
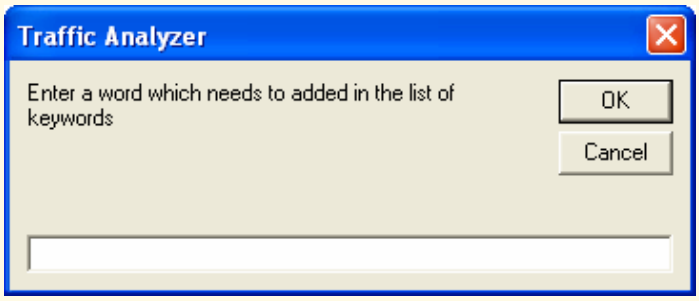
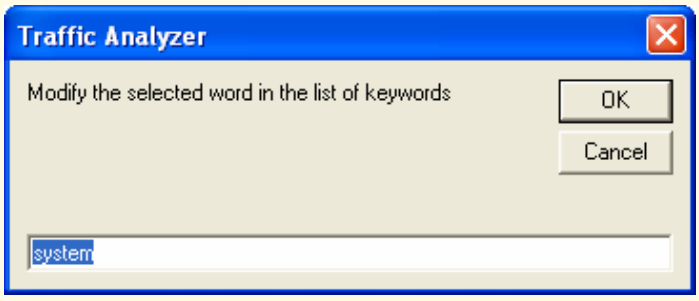
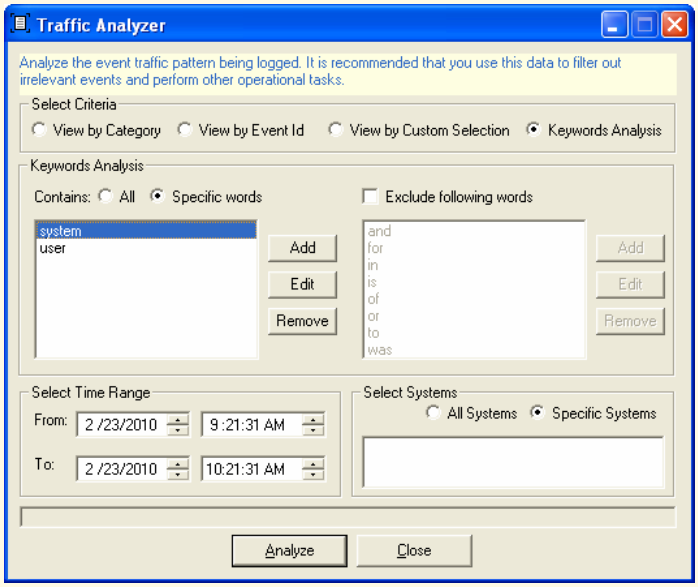
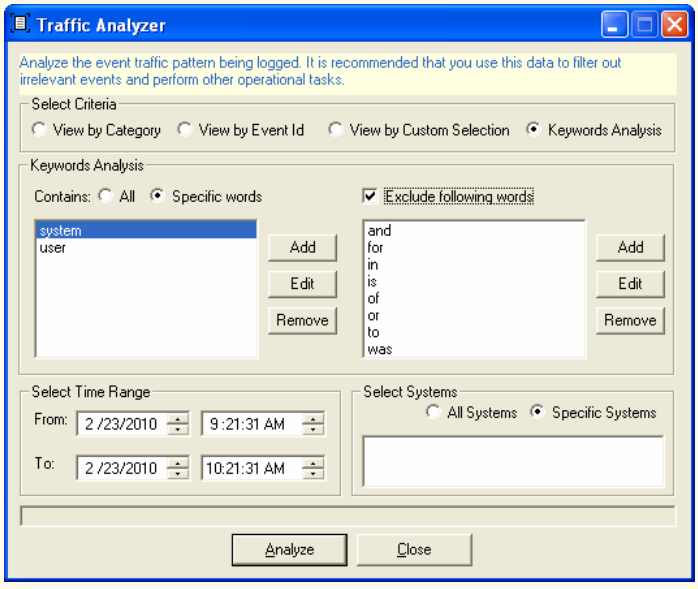


Table 60

Field	Description
Keywords Analysis: Helps to analyze events by keywords.	
Contains All	Analyze logs that contain all keywords specified.

Field	Description
Keywords Analysis: Helps to analyze events by keywords.	
	 Click **Add** to add keywords and then click **OK** on the dialog box. EventTracker adds the new keyword to the list.  Select a keyword from the list and then click Edit to modify the keyword.  Select a keyword from the list and then click Remove to delete from the list.
Contains	Analyze logs that contain selected keywords. Select a keyword

Field	Description
Keywords Analysis: Helps to analyze events by keywords.	
Specific words	in this list and then click **Analyze**. 
Excluding following words	Select this check box to exclude all words specified in this list. You can also add, modify, and delete keywords from this list. 

4 Type appropriately in the relevant fields.

5 Select the systems.

6 Click **Analyze**.

EventTracker displays the report in the Notepad.

Tracking Enterprise Activity

Enterprise Activity module helps you effectively monitor and manage enterprise activities.

It presents statistical data on:

- Alert events occurred.
- Admin & non-Admin user activities.
- Processes executed. Provision to get more information on processes.
- Activities occurred at a particular system/IP address. Provision to resolve IP addresses.
- Event IDs on occurrences. Provision to get more information on Event IDs.

For more information, refer http://www.prismmicrosys.com/Support/latestguides/Enterprise Activity.pdf

Analyzing Alerts

This option helps you analyze Alert events occurred in the monitored systems.

To analyze Alert events

1. Double-click **Alerts Dashboard** on the Control Panel.

   EventTracker displays the Alerts Dashboard.

Figure 317 Alerts Dashboard

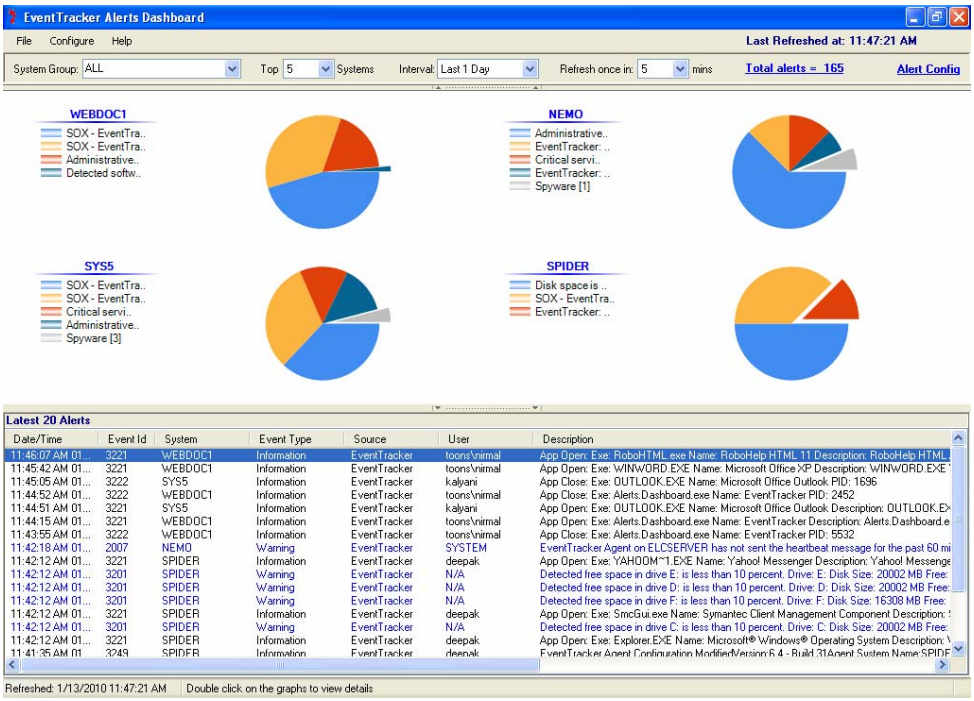
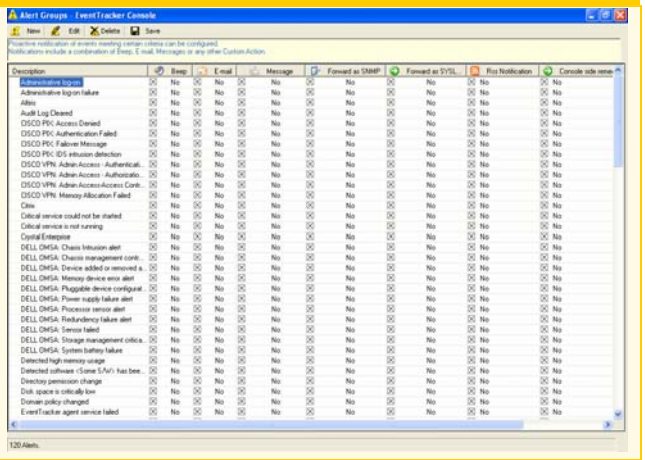


Table 61

Field	Description
System Group	Enterprise system groups are listed in this drop-down list. By default, EventTracker selects the ALL option.
Top	By default, top 5 systems with more Alert events are displayed in the top pane. You can select up to top 20 systems.
Interval	Select the period for which you want to view Alert details.
Refresh once in	Select the refresh interval for both the panes.

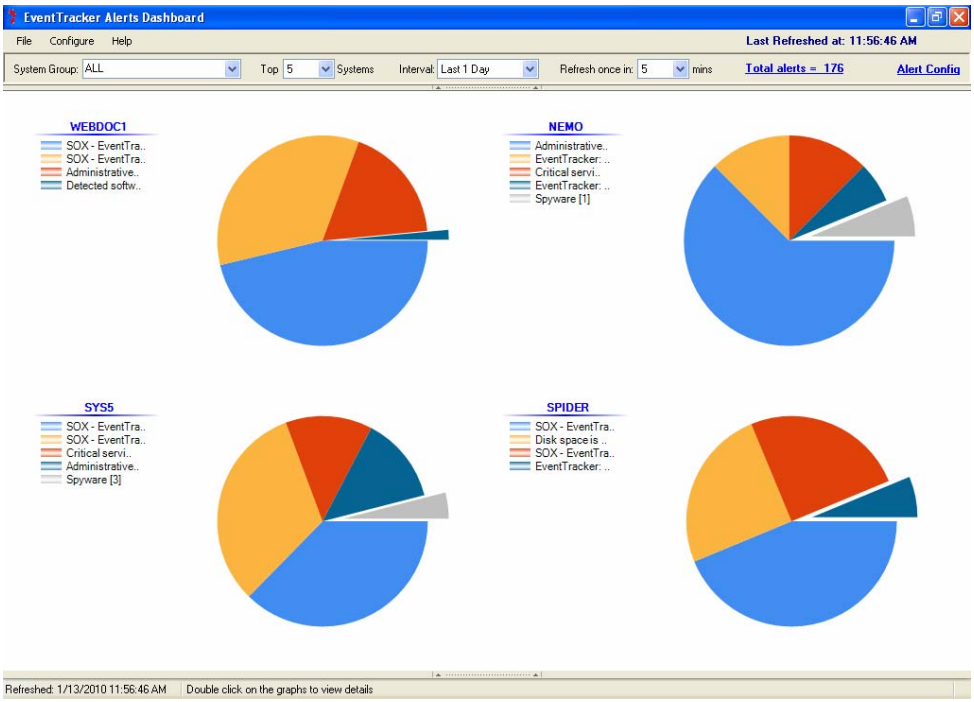
Table 62

Click	To
Total alerts	View all Alert events occurred in all monitored systems.
Alert Config	Open Alert Groups console.

Click	To
	

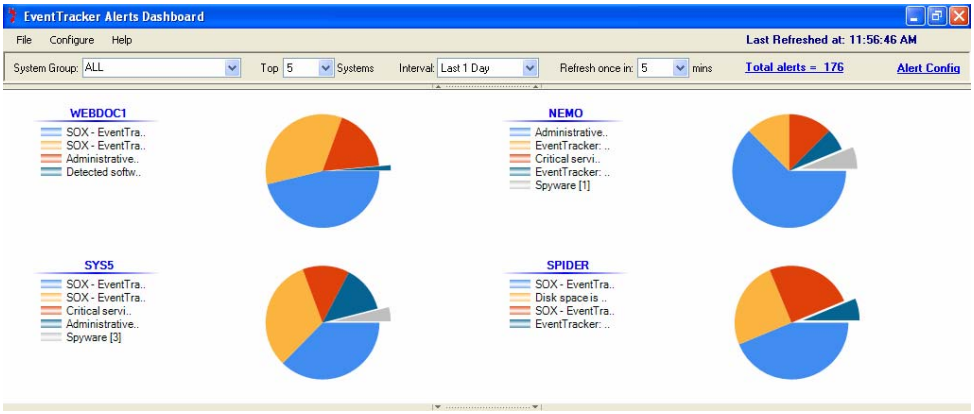
2 Click the collapsible splitter controls to hide the bottom pane to view full view of the graphs.

Figure 318 Full View of Graphs



By default, EventTracker displays the summary of events of top 5 Alert rules of the in the top pane.

Figure 319 Alerts Dashboard – Top Pane

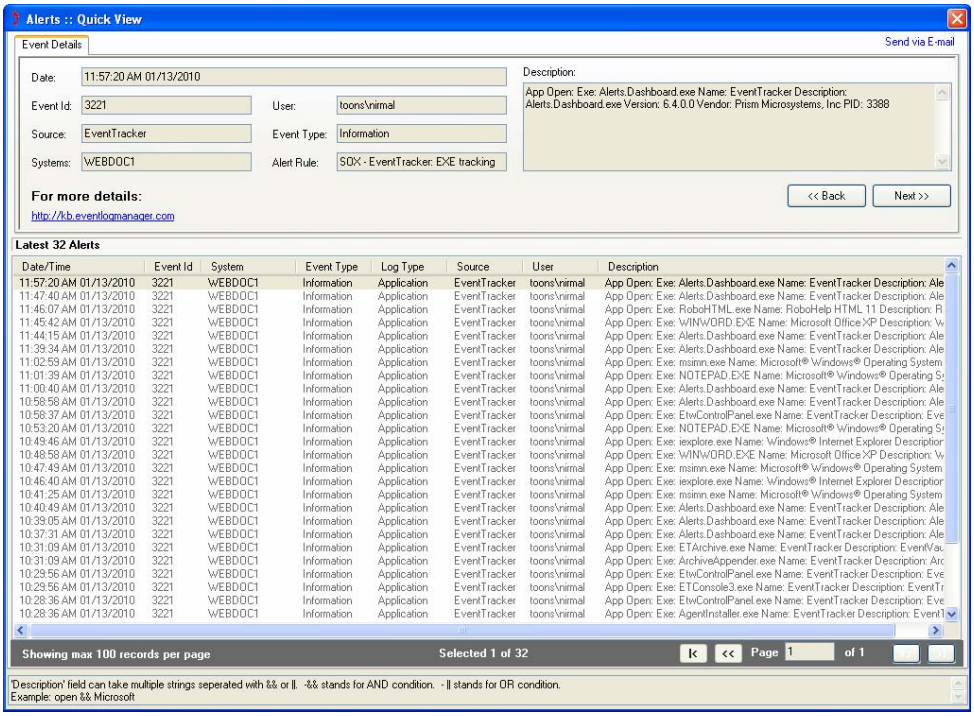


3 Click a legend or a pie to view exploded view of the pie chart.

4 Double-click a legend or a pie on the chart to view Alert details of that particular Alert rule.

EventTracker displays the Alert details in Quick View.

Figure 320 Alerts Details – Quick View



Note

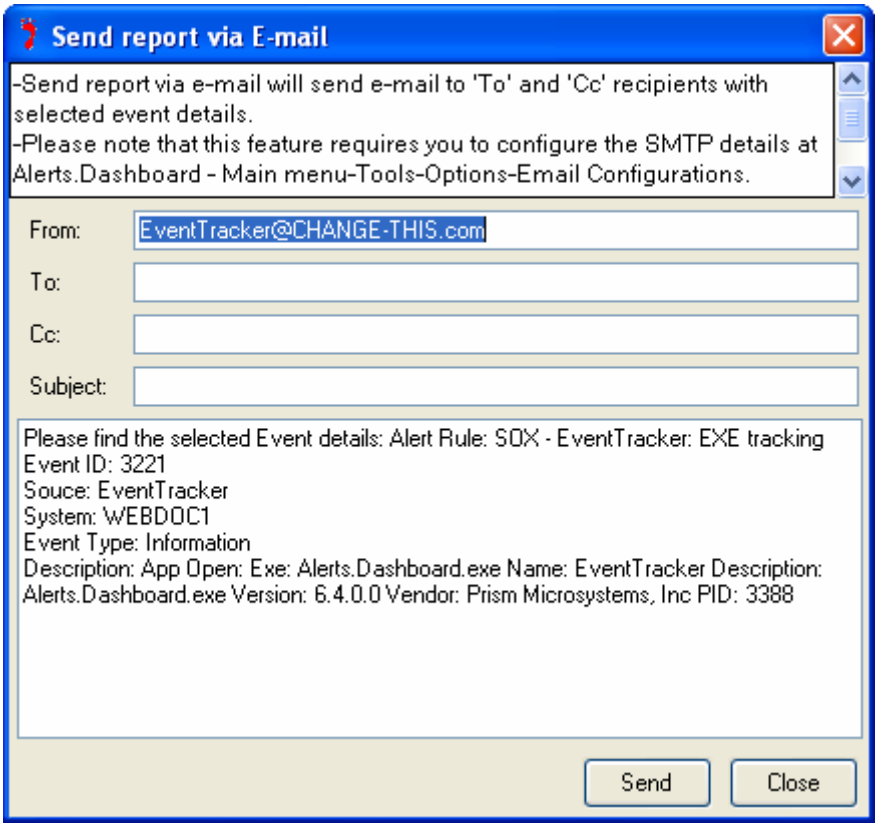
You can e-mail only one Alert detail at once.

5 Click the **Next >>** button to move to the next detail or select a row in the bottom pane.

6 Click the **Send via E-mail** hyperlink at the right-upper corner.

EventTracker displays the Send report via E-mail window.

Figure 321 Send report via E-mail

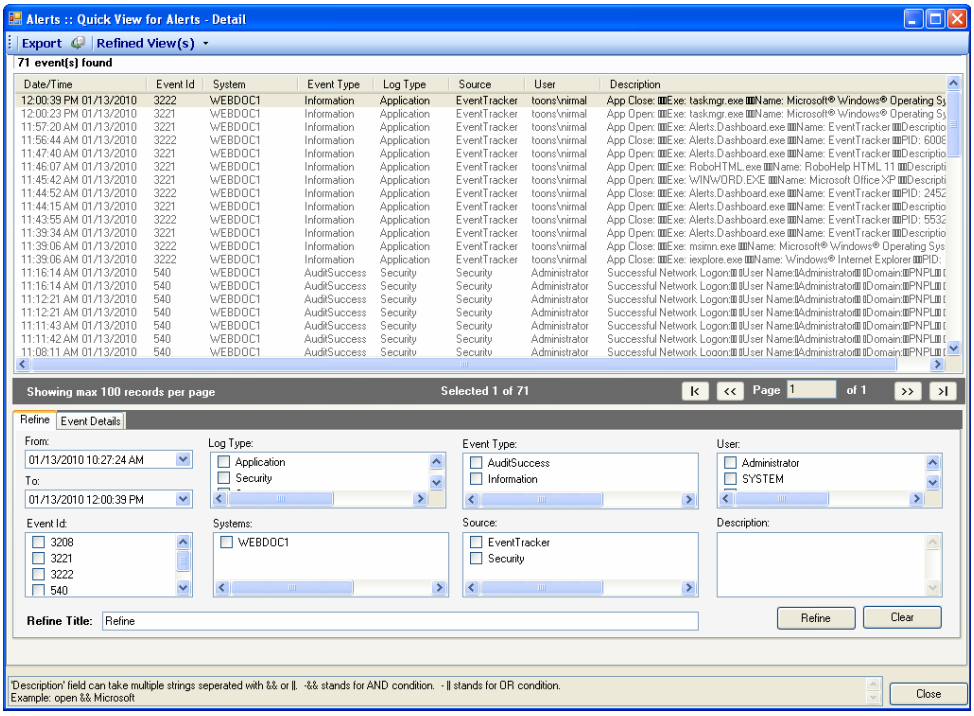

Send report via E-mail
-Send report via e-mail will send e-mail to 'To' and 'Cc' recipients with selected event details.
-Please note that this feature requires you to configure the SMTP details at Alerts.Dashboard - Main menu-Tools-Options-Email Configurations.
From:
EventTracker@CHANGE-THIS.com
To:
Cc:
Subject:
Please find the selected Event details: Alert Rule: SOX - EventTracker: EXE tracking
Event ID: 3221
Souce: EventTracker
System: WEBDOC1
Event Type: Information
Description: App Open: Exe: Alerts.Dashboard.exe Name: EventTracker Description: Alerts.Dashboard.exe Version: 6.4.0.0 Vendor: Prism Microsystems, Inc PID: 3388
Send
Close

7 Type appropriate details in the relevant fields and then click **Send**.

8 Double-click the name of the system on the Alerts Dashboard to view all Alert details of that particular system.

EventTracker displays the Alert details in Quick View.

Figure 322 Alerts Details – Quick View

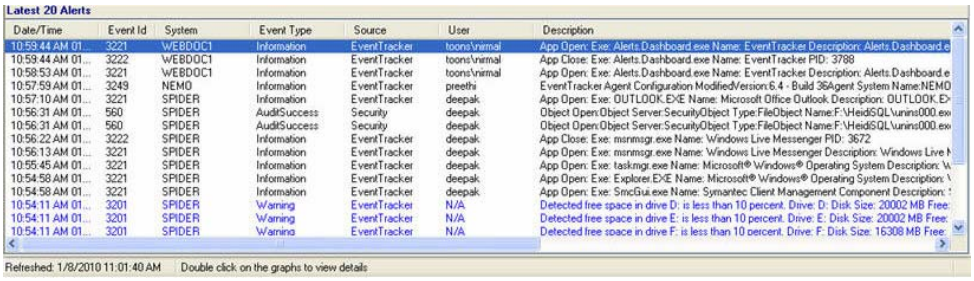


9 Click the **Total alerts** hyperlink in the upper pane to view all Alert event details occurred in all monitored systems.

EventTracker displays the latest 20 Alerts in the bottom pane that occurred in all monitored systems irrespective of the options you have selected in the System Group and Top drop-down lists.

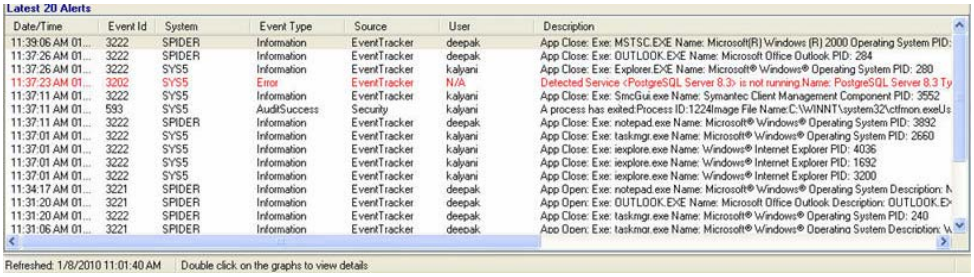
EventTracker highlights the Warning events in "Blue"

Figure 323 Alerts Dashboard – Bottom Pane



EventTracker highlights the Audit Failure events in "Red"

Figure 324 Alerts Dashboard – Bottom Pane



10 Double-click a row to view the details in Quick View.

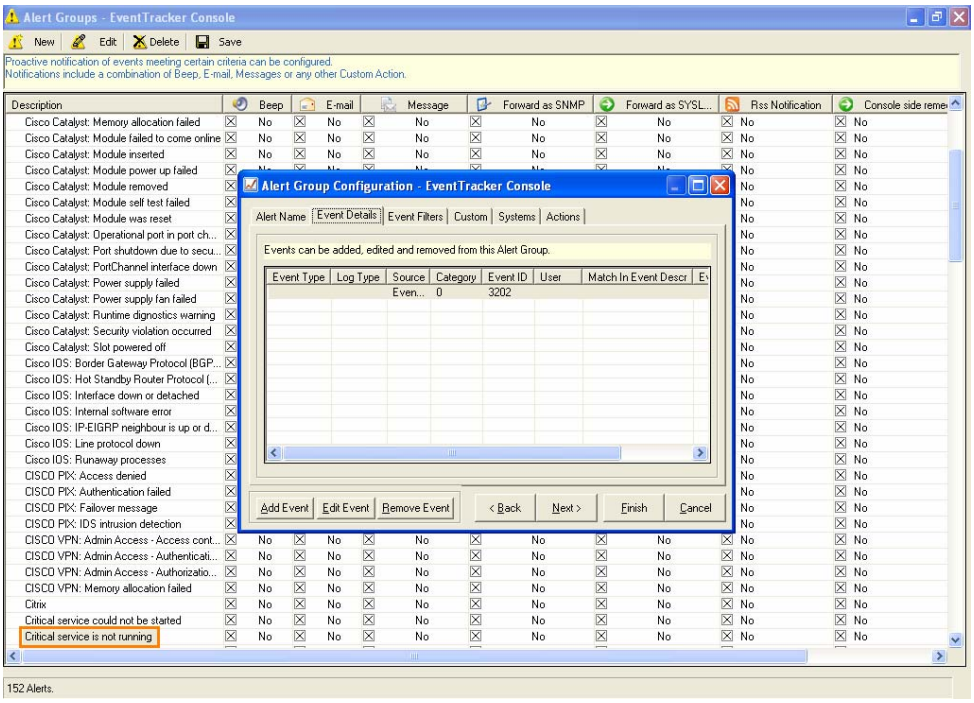
11 Right-click a row to edit the Alert rule.

EventTracker displays the shortcut menu.

12 Form the shortcut menu, choose **Tune this alert**.

EventTracker displays the Alert rule details.

Figure 325 Alert Group Configuration



Chapter 12
Managing Category Groups and Categories

In this chapter, you will learn how to:

- Configure & Manage Category Groups
- Configure & Manage Categories

Managing Category Groups

A set of relevant Categories can be organized under a Group.

Creating Category Groups

This option enables you to organize Category groups where by you can add, delete and modify categories in that Group.

To create a Category Group

1. Open the Management Console.
2. Click the **Configure** menu and select the **Manage Categories** option.

   (OR)

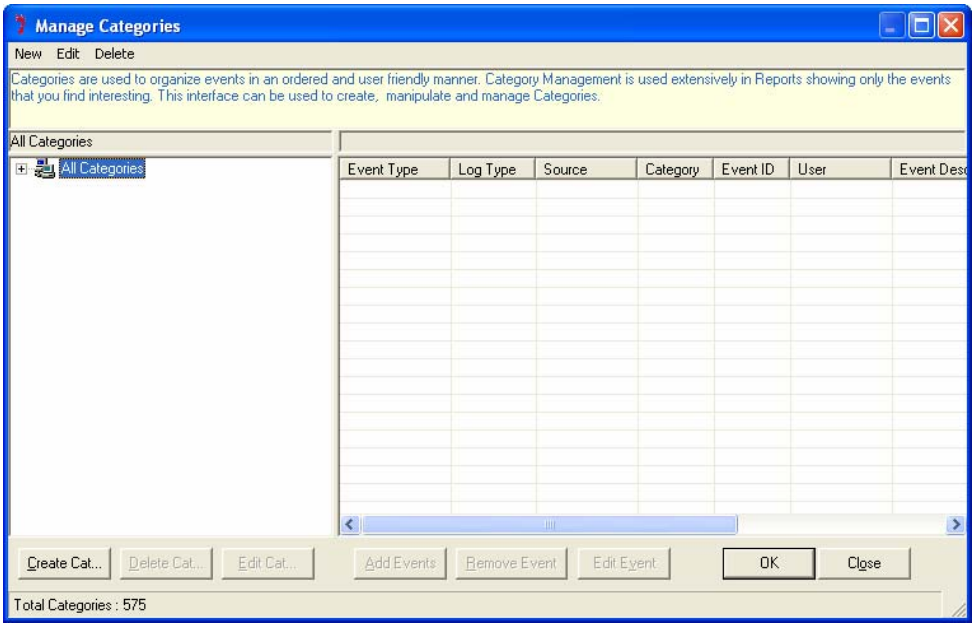
   Right-click any of the Groups or Categories on the left pane.

   EventTracker displays the shortcut menu.

   From the shortcut menu, choose **Manage Categories**.

   EventTracker displays the Manage Categories console.

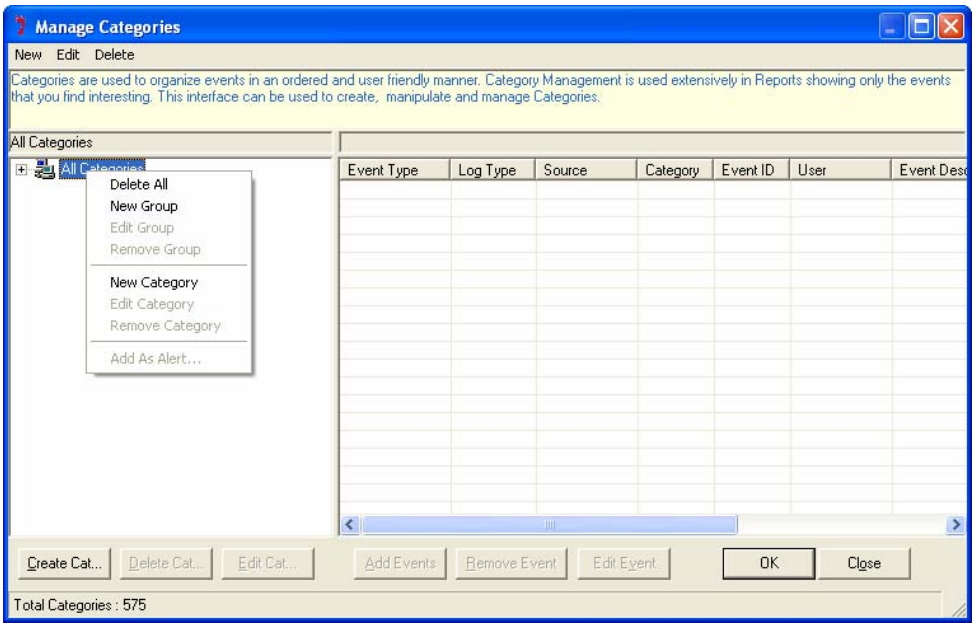
Figure 326 Manage Categories window



3. Right-click **All Categories** or any other Group in the left pane.

   EventTracker displays the shortcut menu.

Figure 327 Manage Categories window



From the shortcut menu, choose **New Group**.

Note

If you select any other pre-defined Group, the new Group you create will be created as a sub group to that selected Group that is indicated in the Add Group dialog box against **Parent node is** label.

(OR)

Click the **New** menu and select the **New Group** option.

EventTracker displays Add Group dialog box.

Figure 328 Add Group dialog box.

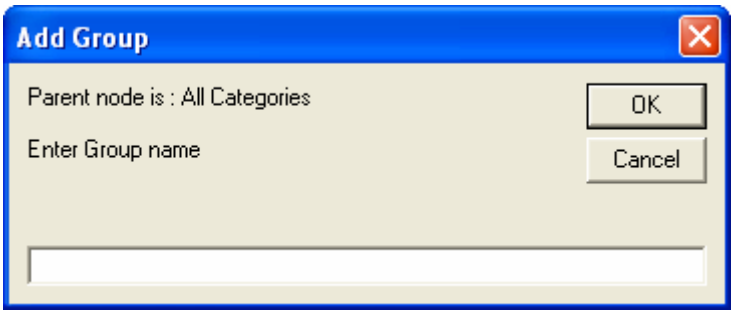
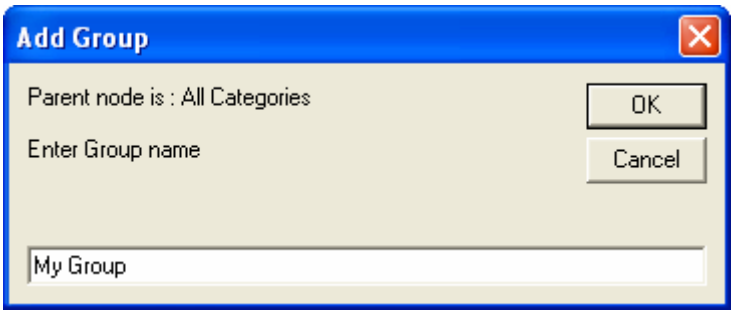


Table 63

Field	Description
Parent node is	Name of the parent group under which the newly created will get added up.
Enter Group name	Name of the Group you create.

4 Type the name of the Group you create in the **Enter Group name** field.

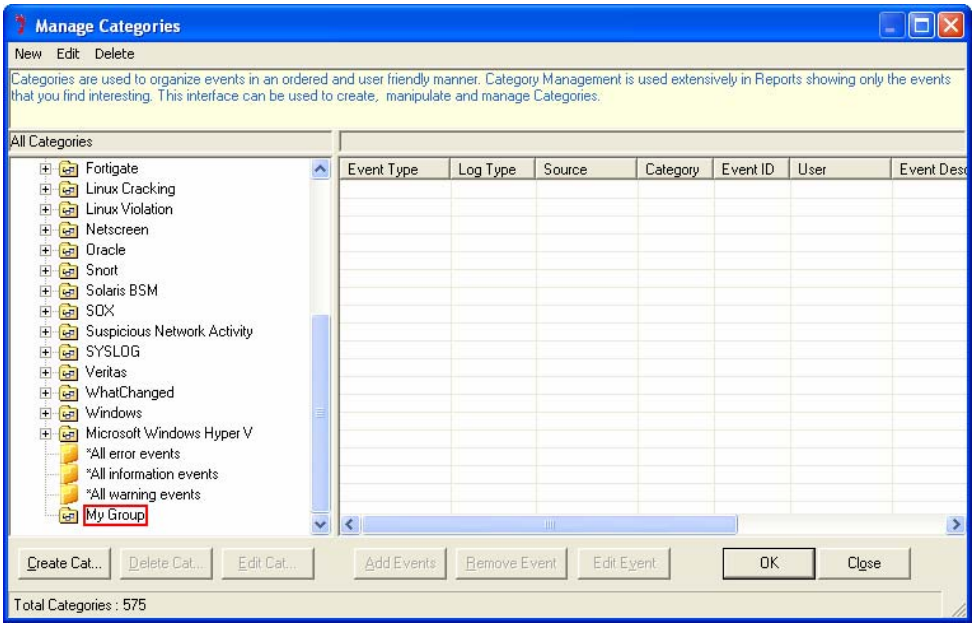
Figure 329 Add Group dialog box.



5 Click **OK**.

6 Expand the tree. EventTracker displays the newly created Group.

Figure 330 Manage Categories dialog box with newly created Group.

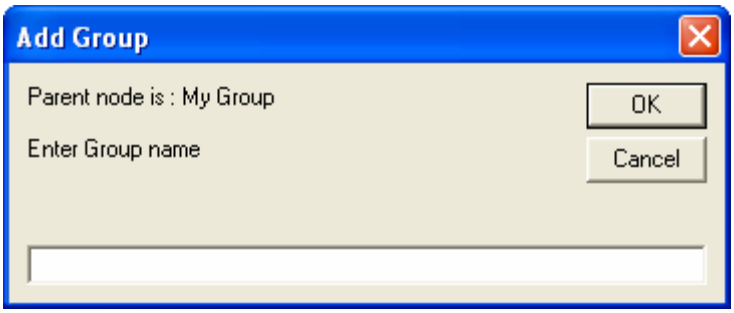


7 To create sub-group within that newly created Group, right-click it.

From the shortcut menu, choose **New Group**.

EventTracker displays Add Group dialog box.

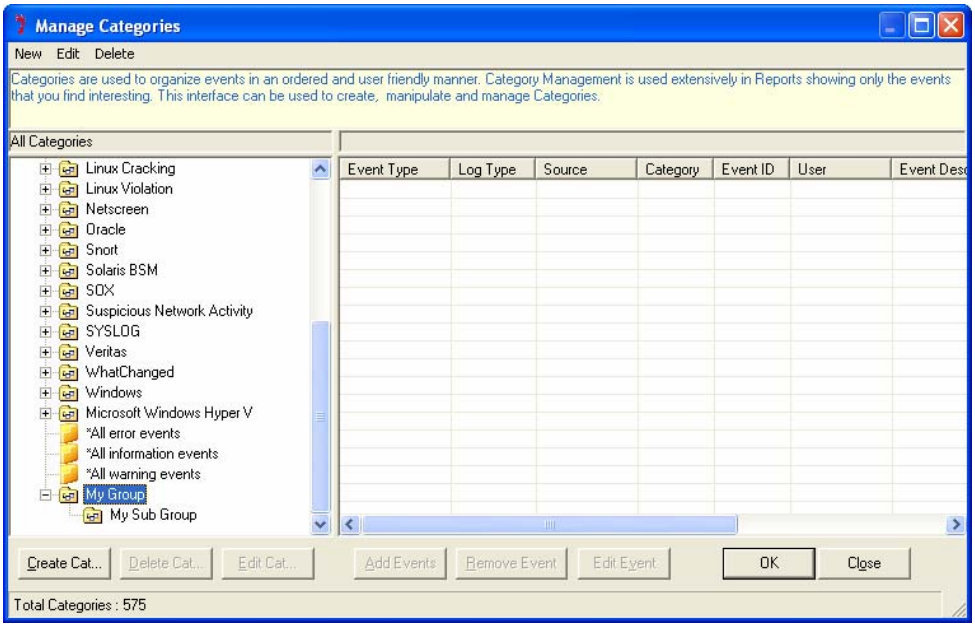
Figure 331 Add Group dialog box.



8 Type the Group name in the **Enter Group name** field and then click **OK**.

EventTracker displays the Manage Categories console with the newly created subgroup.

Figure 332 Manage Categories dialog box with newly created Group.



9 Click **OK**.

10 Open the Management Console.

EventTracker add the newly added Category Group to the All Categories tree.

11 Open the Reports Console.

12 Click Operations tab in the Tree pane.

13 Expand User Defined Category Group.

EventTracker adds the newly added Category Group to this Category Group.

Adding Categories to a Group

This option helps you add Categories to a Category Group

To add Categories to a Category Group

1. Open the Management Console.
2. Right-click the Group in the left pane for which you want to add Categories.

   EventTracker displays the shortcut menu.

   From the shortcut menu, choose **New Category**.

   (OR)

   Open **Manage Categories** console.

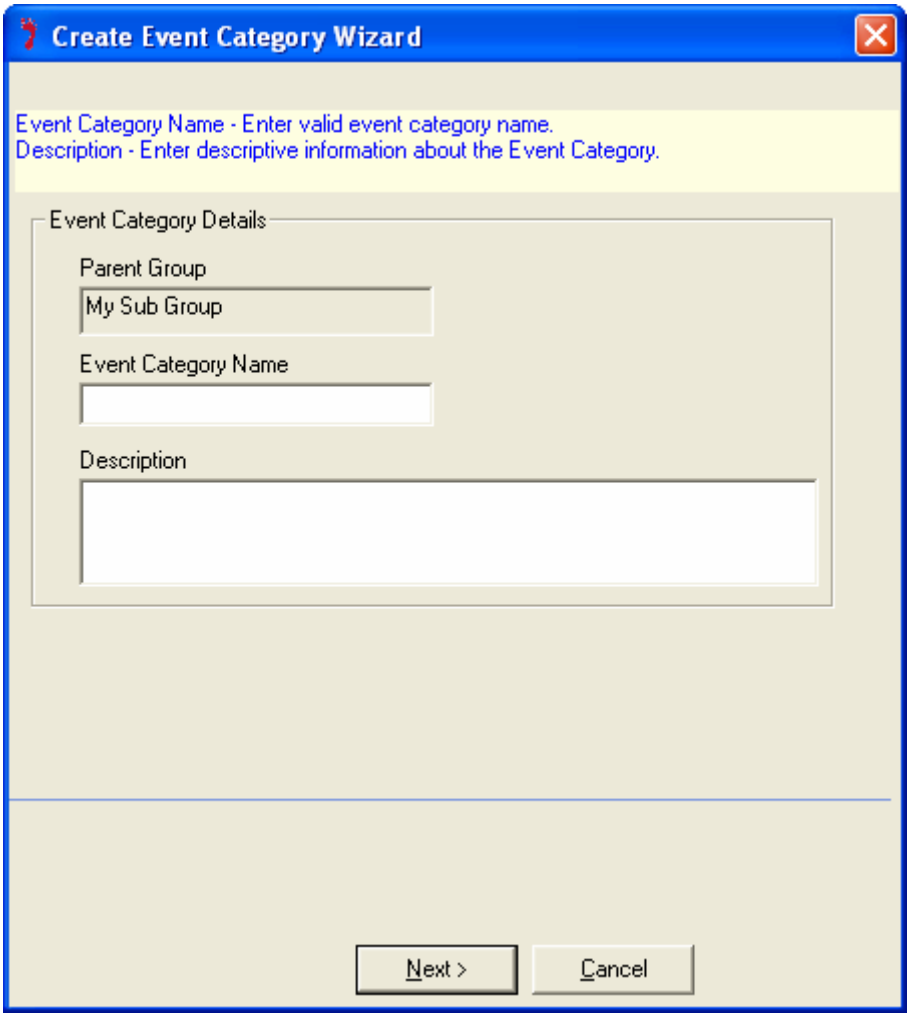
   Select the Group in the tree for which you want to add Categories.

   Right-click it. EventTracker displays the shortcut menu.

   From the shortcut menu, choose **New Category**. (OR) click the **New** menu and select the **New Category** option (OR) click **Create Cat**

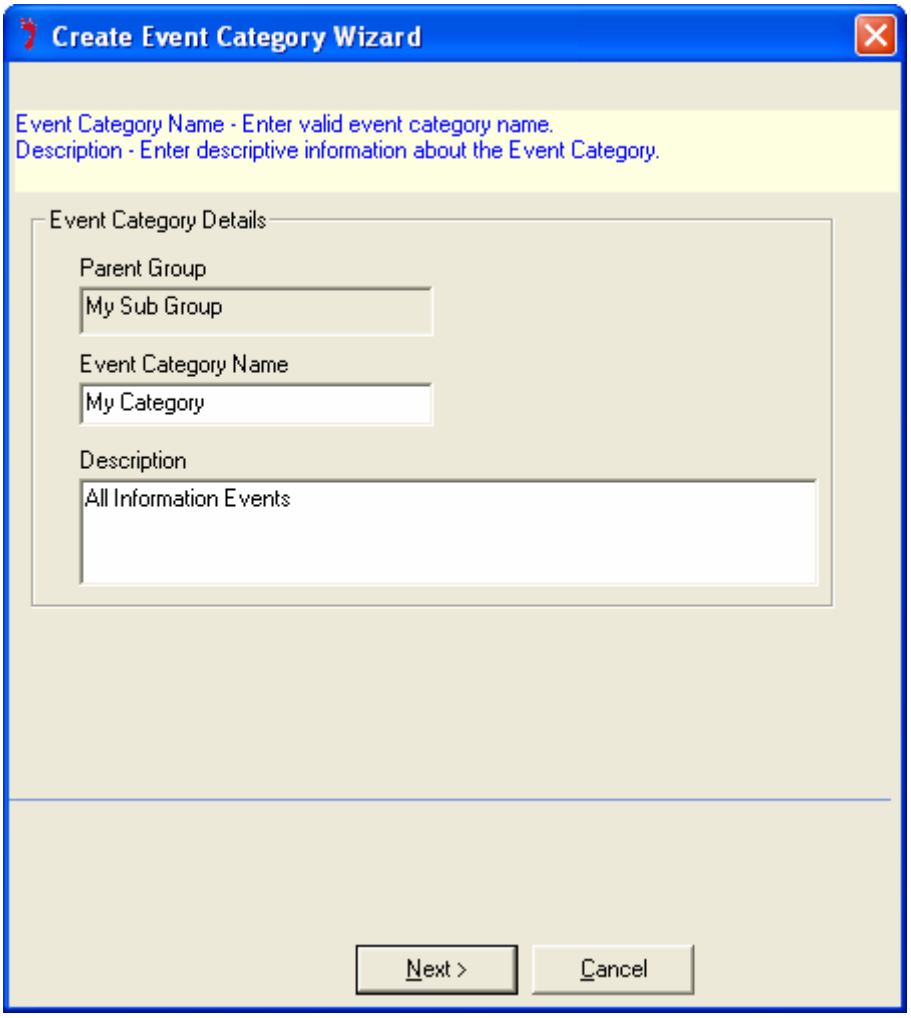
   EventTracker displays the Create Event Category Wizard.

Figure 333 Create Event Category Wizard.



3 Type appropriately in the relevant fields.

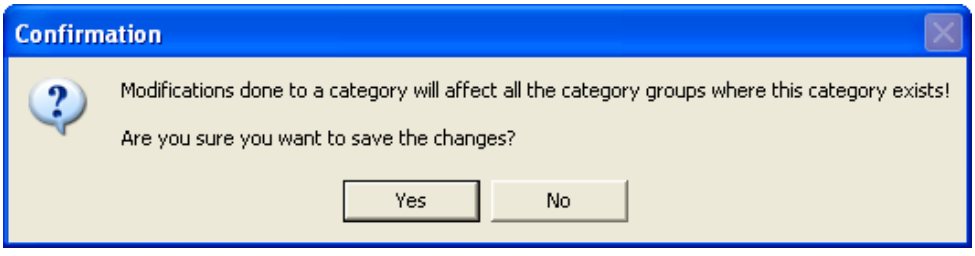
Figure 334 Create Event Category Wizard.



4 Click **Next>**.

EventTracker displays the Confirmation message box.

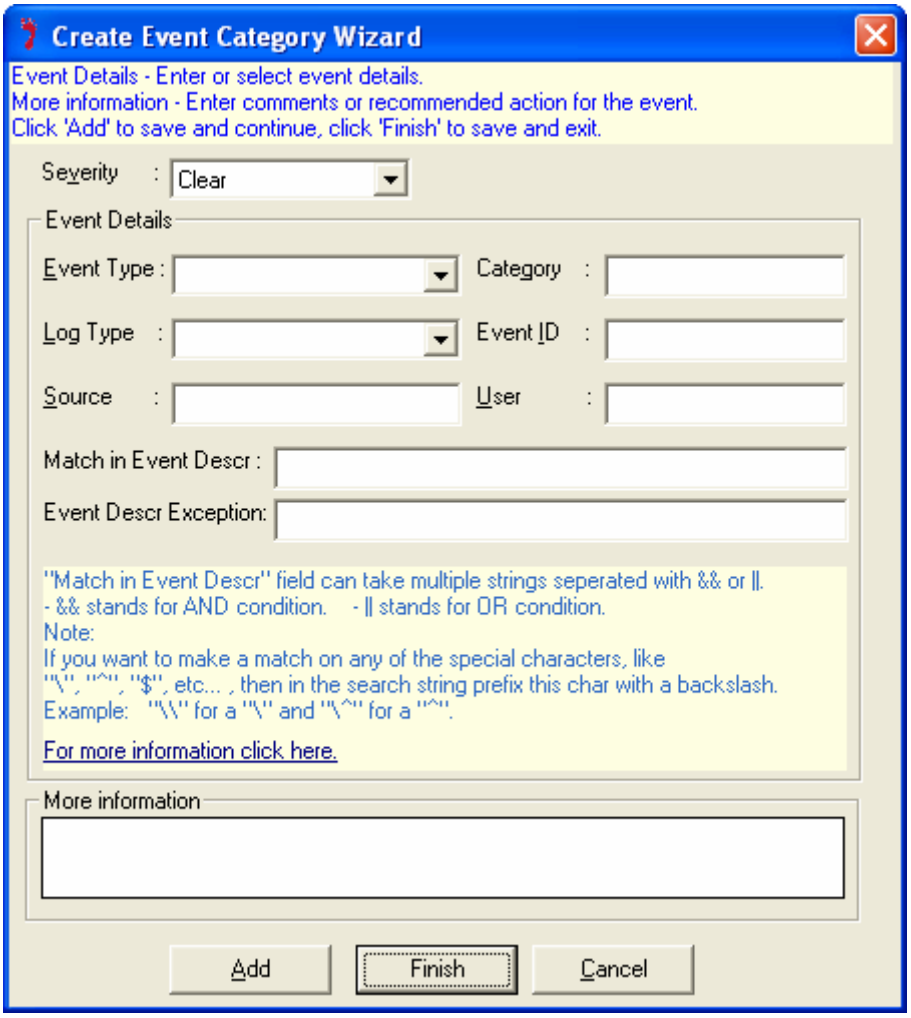
Figure 335 Confirmation message box.


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

5 Click **Yes**.

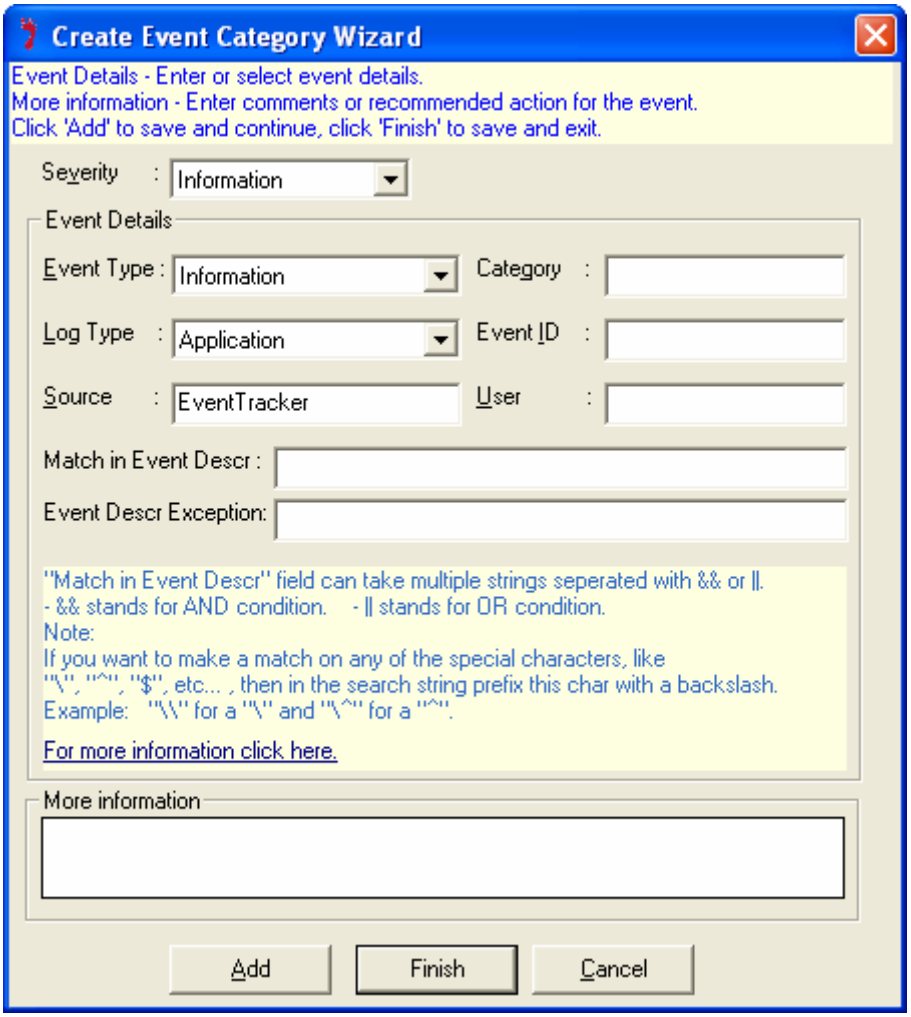
EventTracker displays the Create Event Category Wizard.

Figure 336 Create Event Category Wizard.


Create Event Category Wizard
Event Details - Enter or select event details.
More information - Enter comments or recommended action for the event.
Click 'Add' to save and continue, click 'Finish' to save and exit.
Severity : Clear
Event Details
Event Type :
Category :
Log Type :
Event ID :
Source :
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
Add
Finish
Cancel

6 Type appropriately in the relevant fields.

Figure 337 Create Event Category Wizard.

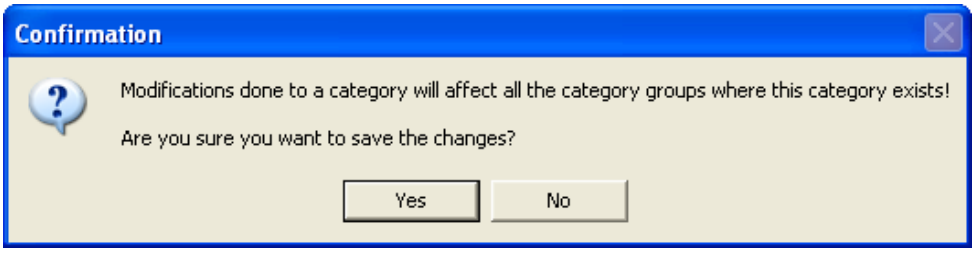

Create Event Category Wizard
Event Details - Enter or select event details.
More information - Enter comments or recommended action for the event.
Click 'Add' to save and continue, click 'Finish' to save and exit.
Severity : Information
Event Details
Event Type : Information
Category :
Log Type : Application
Event ID :
Source : EventTracker
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
Add
Finish
Cancel

7 Click **Add**.

8 Click **Finish**.

EventTracker displays the Confirmation message box.

Figure 338 Confirmation message box.


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

9 Click **Yes**.

EventTracker displays the Manage Categories console.

10 Click **OK**.

EventTracker displays the EventTracker Management Console with newly created Category and its associated events.

Modifying Category Groups

This option enables you to modify a Category Group.

To modify a Category Group

1 Open the Management Console.

2 Click the **Configure** menu and select the **Manage Categories** option.

(OR)

Right-click any of the Groups or Categories on the left pane.

EventTracker displays the shortcut menu.

From the shortcut menu choose **Manage Categories**.

EventTracker displays the Manage Categories console.

3 Expand the tree in the left pane.

4 Right-click the Group that you want to modify.

EventTracker displays the shortcut menu.

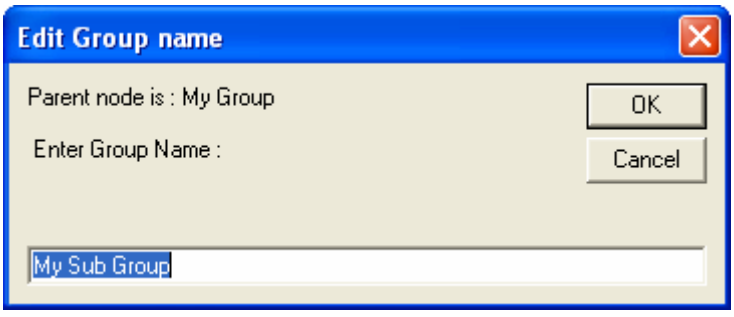
From the shortcut menu, choose **Edit Group**.

(OR)

Click the **Edit** menu and select the **Edit Group** option.

EventTracker displays the Edit Group name dialog box.

Figure 339 Edit Group name dialog box.



5 Type appropriate Group name in the **Enter Group name** field and then click **OK**.

Deleting Category Groups

This option enables you to remove a Category Group.

To remove a Category Group

1. Open the Management Console.
2. Click the **Configure** menu and select the **Manage Categories** option.

   (OR)

   Right-click any of the Groups or Categories on the left pane.

   EventTracker displays the shortcut menu.

   From the shortcut menu choose **Manage Categories**.

   EventTracker displays the Manage Categories console.
3. Expand the tree in the left pane.
4. Right-click the Group that you want to delete.

   EventTracker displays the shortcut menu.

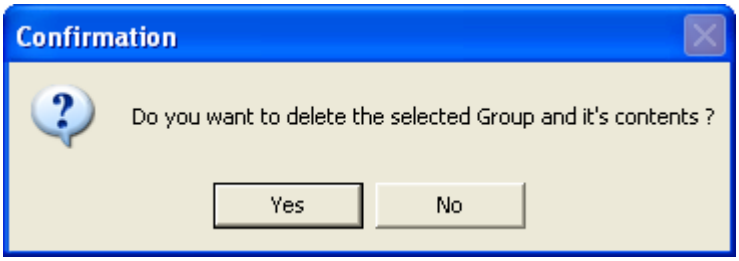
   From the shortcut menu, choose **Remove Group**.

   (OR)

   Click the **Delete** menu and select the **Delete Group** option.

   EventTracker displays the Confirmation message box.

Figure 340
Confirmation message box.



5. Click **Yes** to remove or **No** to abort.

Managing Event Categories

A set of relevant events can be grouped under a Category. For example, you can create a set of MS-Exchange events under one Category and use this Category to show all events that occurred in MS-Exchange. This is far easier and flexible than generic reports.

Creating Event Categories

This option enables you to organize categories in an ordered manner. You can create, modify and delete the categories.

To create a Category

1. Open the Management Console.
2. Click the **Configure** menu and select the **Manage Categories** option

   (OR)

   Right-click any of the Groups or Categories on the left pane.

   EventTracker displays the shortcut menu.

   From the shortcut menu, choose **Manage Categories**.

   EventTracker displays the Manage Categories console.
3. Click **Create Category**.

   (OR)

   Click the **New** menu and select the **New Category** option.

   (OR)

   Right-click All Categories.

   EventTracker displays the shortcut menu.

   From the shortcut menu, choose **New Category**.

   EventTracker displays the Create Event Category Wizard.

Figure 341 Create Event Category dialog box

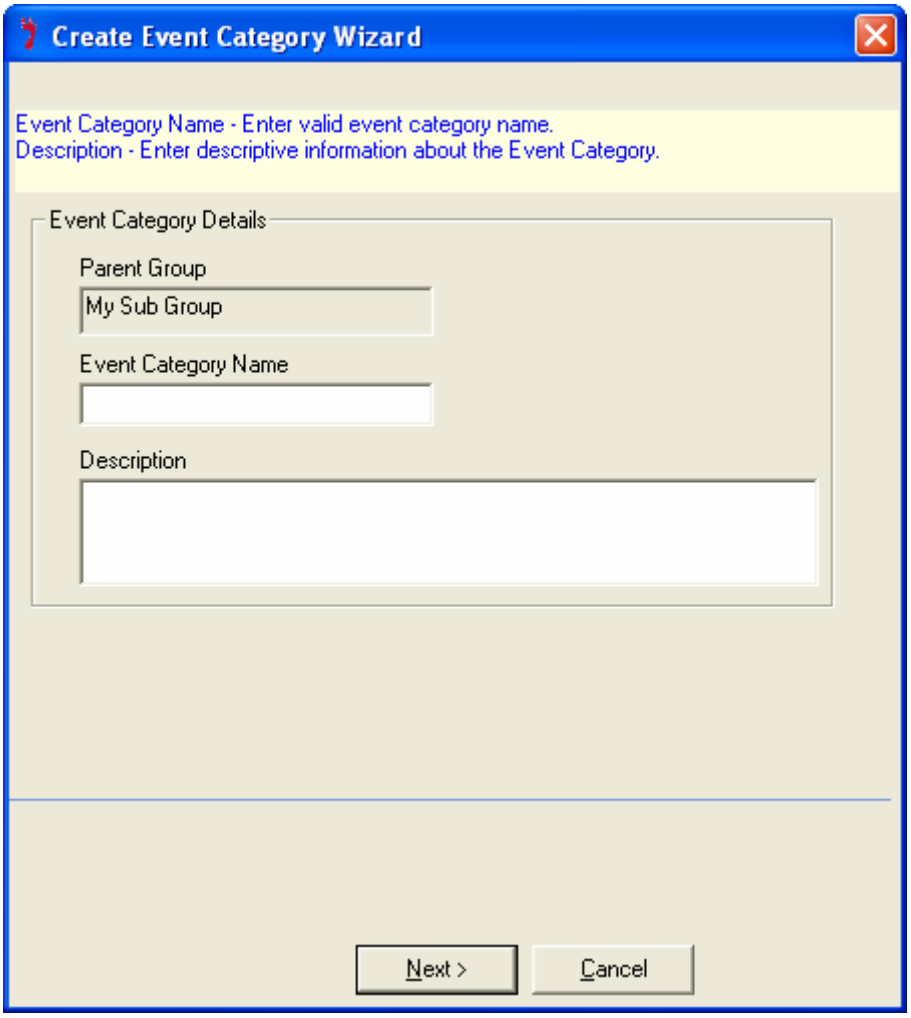


Table 64

Field	Description
Parent Group	The parent node under which the new category is created.
Event Category Name	Type the event category name in this field.
Description	Type the event category description in this field.

(OR)

Right-click any of the nodes in the left pane of the Management Console.

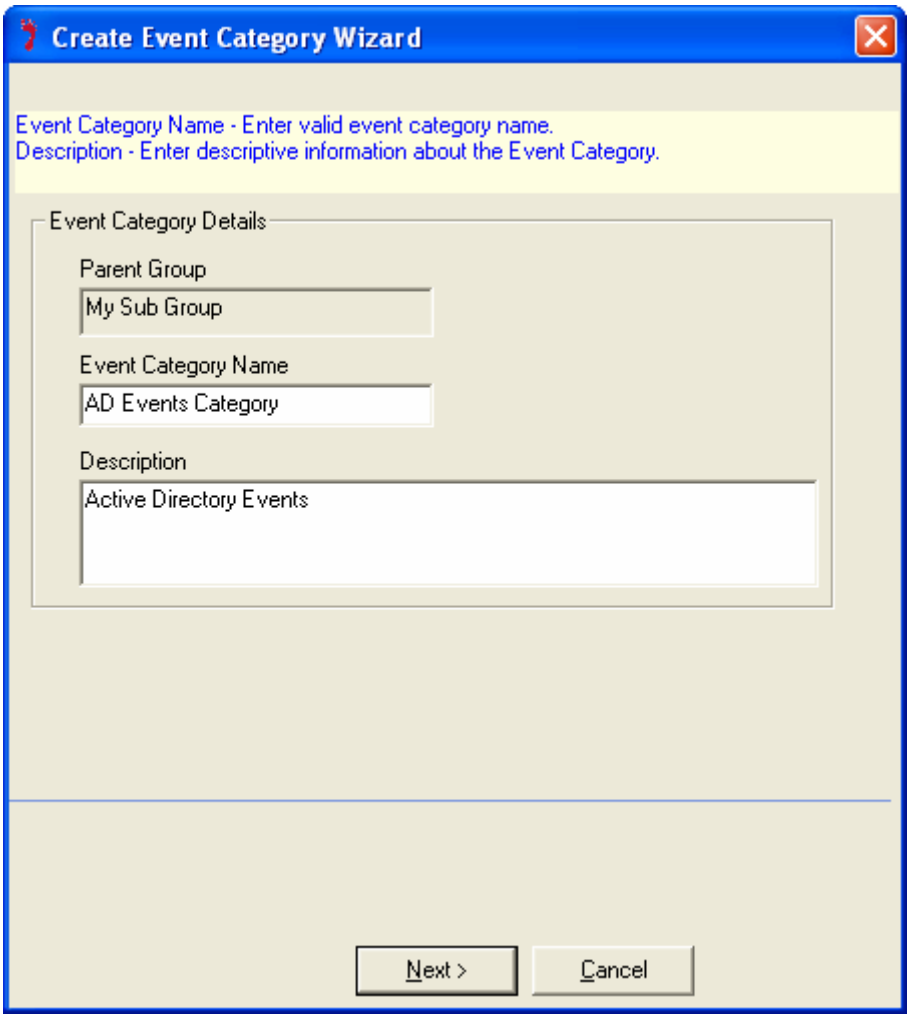
EventTracker displays the shortcut menu.

From the shortcut menu, choose **New Category**.

EventTracker displays the Create Event Category Wizard

4 Type appropriately in the relevant fields.

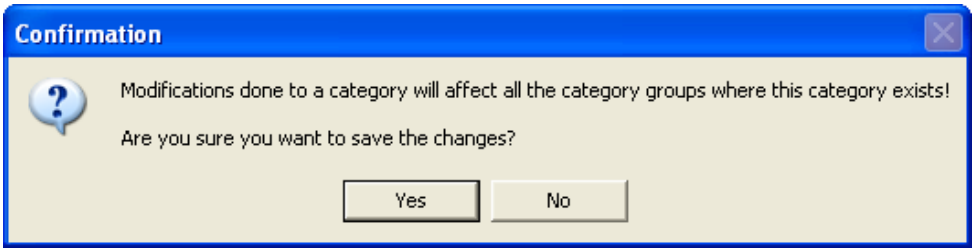
Figure 342 Create Event Category dialog box



5 Click **Next>**.

EventTracker displays the Confirmation message box.

Figure 343 Confirmation message box


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

6 Click **Yes**.

EventTracker displays the Create Event Category Wizard dialog box.

Figure 344 Create Event Category dialog box

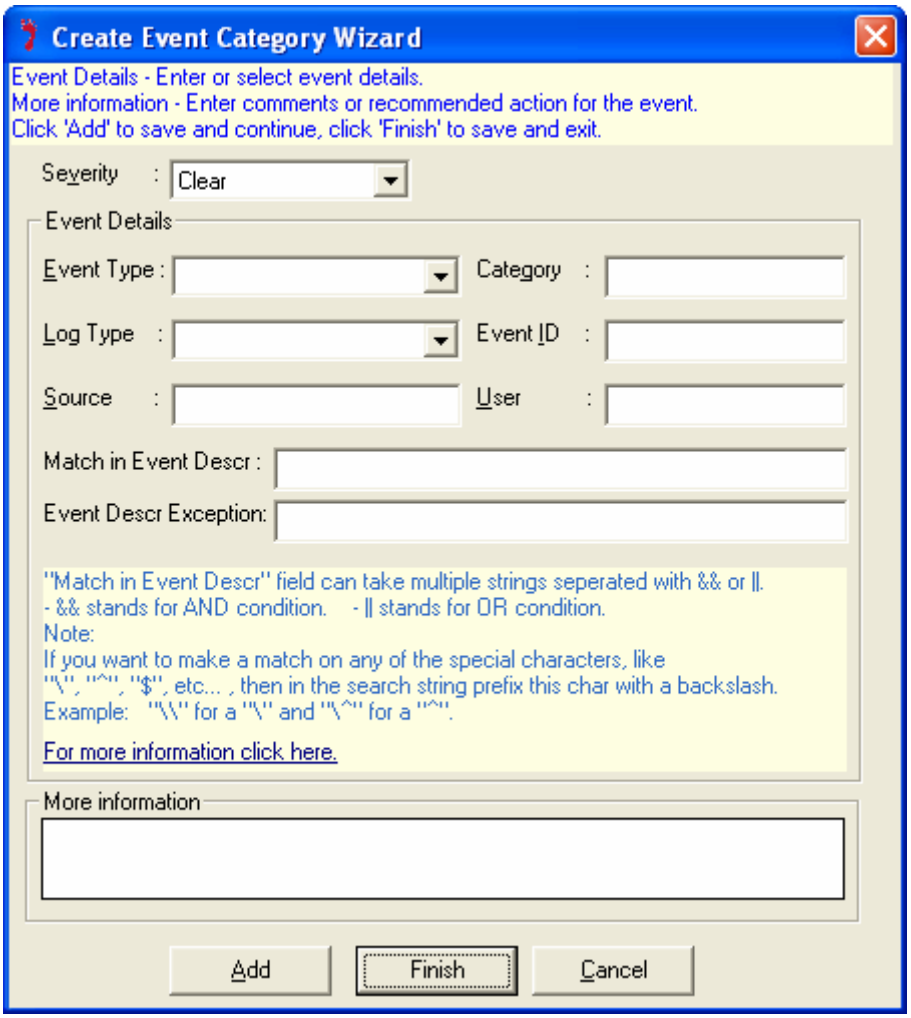

Create Event Category Wizard
Event Details - Enter or select event details.
More information - Enter comments or recommended action for the event.
Click 'Add' to save and continue, click 'Finish' to save and exit.
Severity : Clear
Event Details
Event Type :
Category :
Log Type :
Event ID :
Source :
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
Add
Finish
Cancel

Table 65

Field	Description
Severity	Select a severity type from the drop-down list. The options are Clear, Information, Warning, Minor, Major, and Critical.
Event Details	
Event Type	Select an event type from the drop-down list. The options are Error, Warning, Information, Audit Success, Audit Failure, and Success.
Category	Type the category number in this field. This field supports numeric data type only.
Log Type	Select a log type from the drop-down list.

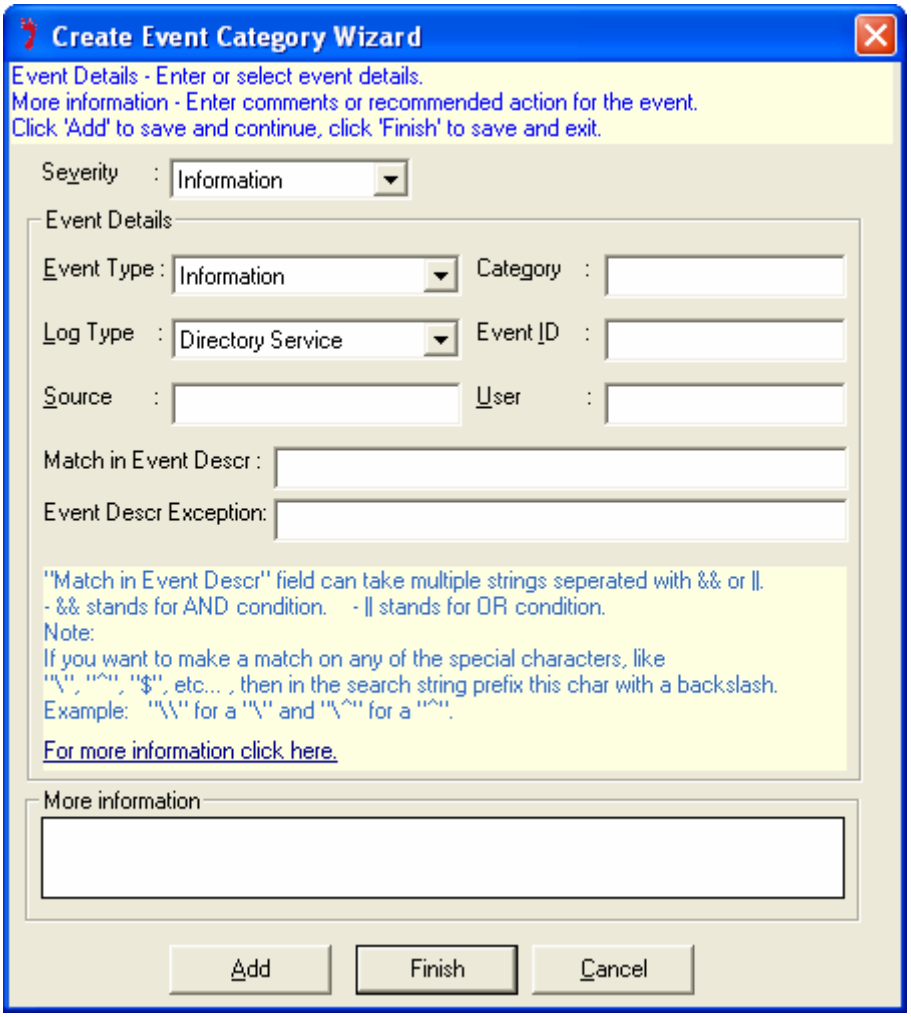
Field	Description
	The options are System, Security, Application, DNS Server, File Replication Service and Directory Service.
Event ID	Type the event ID number in this field. This field supports numeric data type only.
Source	Type the source in this field.
User	Type the user name in this field.
Match in Event Descr.	Type a sub-string of the description that needs to be matched.
More information	Type the additional information about the event category in this field.

Note

If a field is left blank, a wildcard match for that field is assumed. For example, leaving the user field blank implies that any value in that field is acceptable.

7 Type appropriately in the relevant fields.

Figure 345 Create Event Category dialog box

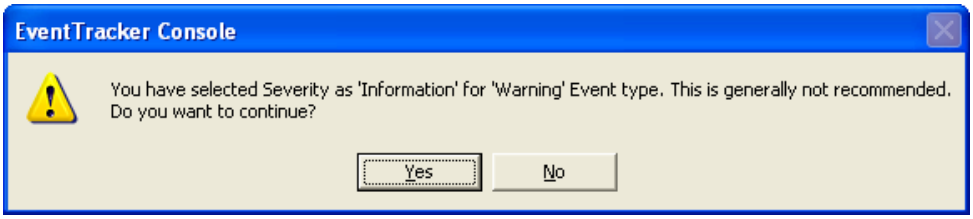

Create Event Category Wizard
Event Details - Enter or select event details.
More information - Enter comments or recommended action for the event.
Click 'Add' to save and continue, click 'Finish' to save and exit.
Severity : Information
Event Details
Event Type : Information
Category :
Log Type : Directory Service
Event ID :
Source :
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
Add
Finish
Cancel

8 Click **Add**.

9 Click **Finish**.

If there is a mismatch in the **Severity** and **Event Type**, then the EventTracker displays the EventTracker Console message box.

Figure 346 Create Event Category dialog box


EventTracker Console
You have selected Severity as 'Information' for 'Warning' Event type. This is generally not recommended.
Do you want to continue?
Yes
No

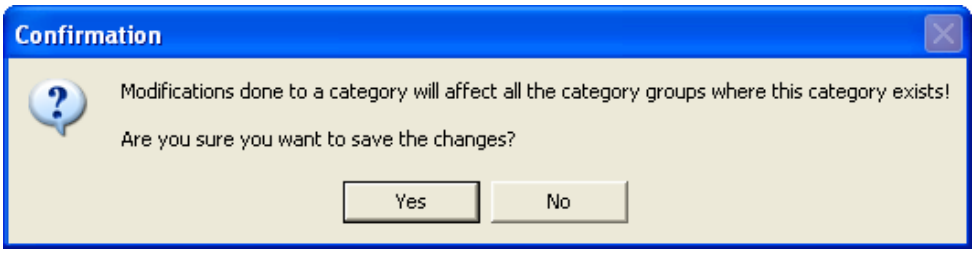
10 Click **Yes** to proceed further or **No** to revert to the Create Event Category Wizard dialog box.

11 Click **Finish**.

> **Note**
>
> You can create Categories without adding any events to that category, which you can add later on by clicking **Add Events** on the **Manage Categories** dialog box.

EventTracker displays the Confirmation message box.

Figure 347
Confirmation message box


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

12 Click **Yes**.

EventTracker displays the Manage Categories console.

Modifying Categories

This option helps you modify Categories.

To modify a category

1 Open the **Manage Categories** dialog box.

(OR)

Right-click the category in the left pane of the **EventTracker Management Console**.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Edit Category**.

EventTracker displays the Manage Categories console.

2 Select the category that you want to modify in the left pane.

3 Click **Edit Category**

(OR)

Right-click the category that you want to modify.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Edit Category**.

(OR)

Click the **Edit** menu and select the **Edit Category** option.

EventTracker displays the Edit Event Category dialog box.

Figure 348 Edit Event Category dialog box

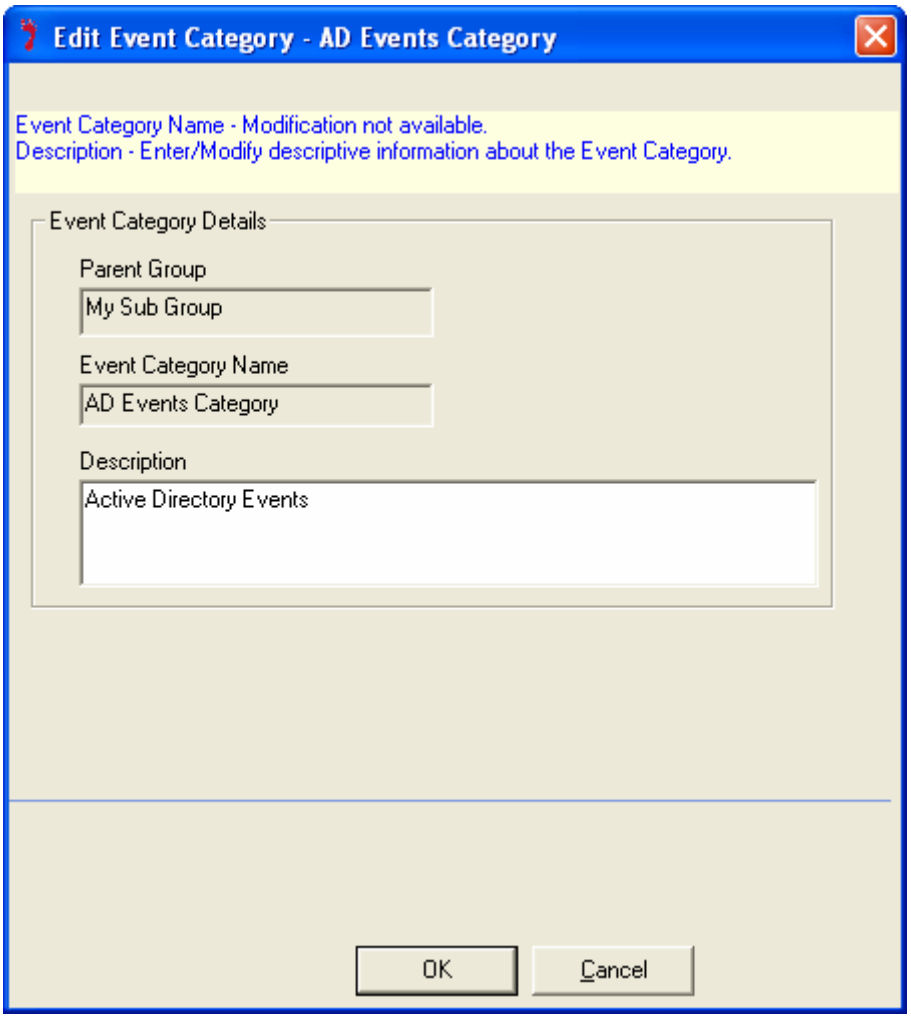


Table 66

Field	Description
Parent Group	The parent node under which the new Category was created.
Event Category Name	This field displays the event category name. This field is not editable.

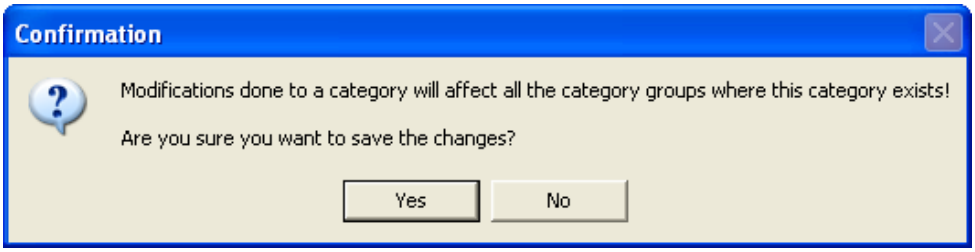
Field	Description
Description	Type the event category description in this field.

4 Type the description you want to modify in the **Description** field.

5 Click **OK**.

EventTracker displays the Confirmation message box.

Figure 349
Confirmation message box


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

6 Click **Yes**.

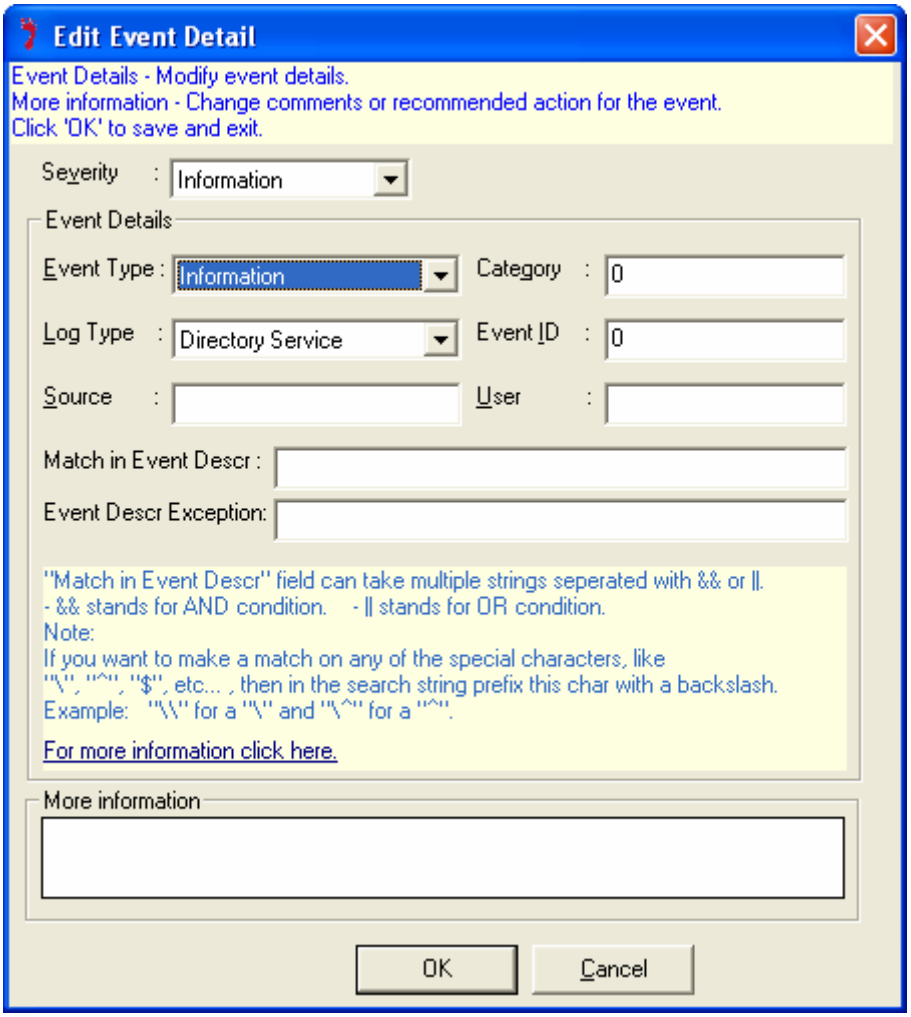
7 To edit event details, double-click the event on the right pane.

(OR)

Select an event and then click **Edit Event**.

EventTracker displays the Edit Event Detail dialog box.

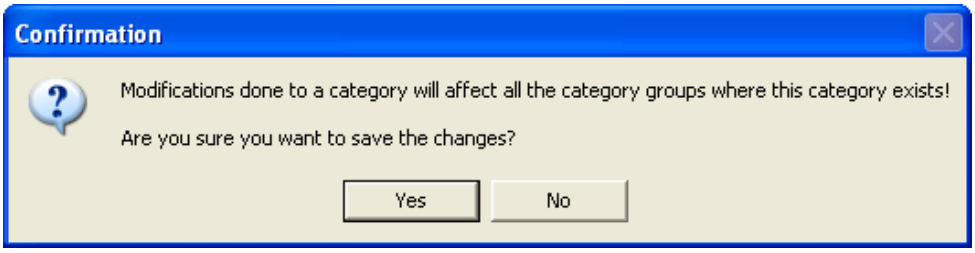
Figure 350 Edit Event Detail dialog box


Edit Event Detail
Event Details - Modify event details.
More information - Change comments or recommended action for the event.
Click 'OK' to save and exit.
Severity : Information
Event Details
Event Type : Information
Category : 0
Log Type : Directory Service
Event ID : 0
Source :
User :
Match in Event Descr :
Event Descr Exception:
"Match in Event Descr" field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note:
If you want to make a match on any of the special characters, like
"\", "^", "$", etc... , then in the search string prefix this char with a backslash.
Example: "\\" for a "\" and "\^" for a "^".
For more information click here.
More information
OK
Cancel

8 Edit appropriately and the click **OK**.

EventTracker displays the Confirmation message box.

Figure 351 Confirmation message box


Confirmation
Modifications done to a category will affect all the category groups where this category exists!
Are you sure you want to save the changes?
Yes
No

9 Click **Yes**.

10 Click **OK** on the Manage Categories console.

Deleting Categories

This option enables you to delete a Category

To delete a Category

1. Open the Manage Categories console.
2. Select the category you want to delete in the left pane.
3. Click **Delete Category**.

   (OR)

   Right-click the category that you want to delete.

   EventTracker displays the shortcut menu.

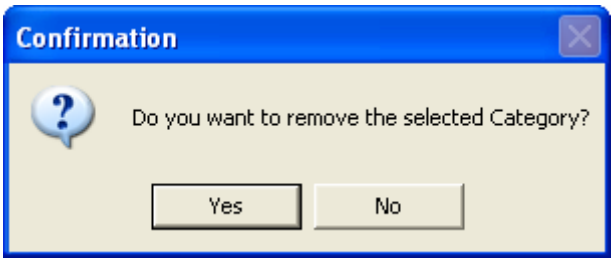
   From the shortcut menu, choose **Remove Category**.

   (OR)

   Click the **Delete** menu and select the **Delete Category** option.

   EventTracker displays the Confirmation message box.

Figure 352 Delete Category – confirmatory message box



4. Click **Yes**.

   EventTracker deletes the selected Category.

Deleting Event Details

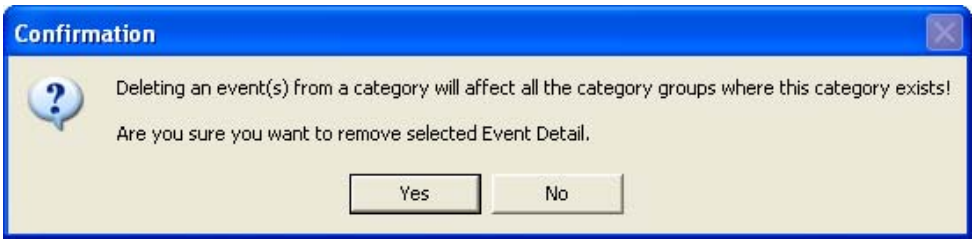
This option helps you delete Event Details.

To delete event details

1. Open the Manage Categories console.
2. Select the category in the left pane.
3. Select the event you want to delete from the displayed list in the right pane.
4. Click **Remove Event**.

EventTracker displays the Confirmation message box.

Figure 353 Delete Event – confirmatory message box


Confirmation
Deleting an event(s) from a category will affect all the category groups where this category exists!
Are you sure you want to remove selected Event Detail.
Yes
No

5 Click **Yes**.

The selected event details are deleted.

Adding Categories as Alerts

This option enables you to add Categories as Alerts

To add Categories as Alerts

1 Open the Management Console.

2 Right-click the Category that you want to configure as Alert.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Add As Alert**

(OR)

Open the Manage Categories console.

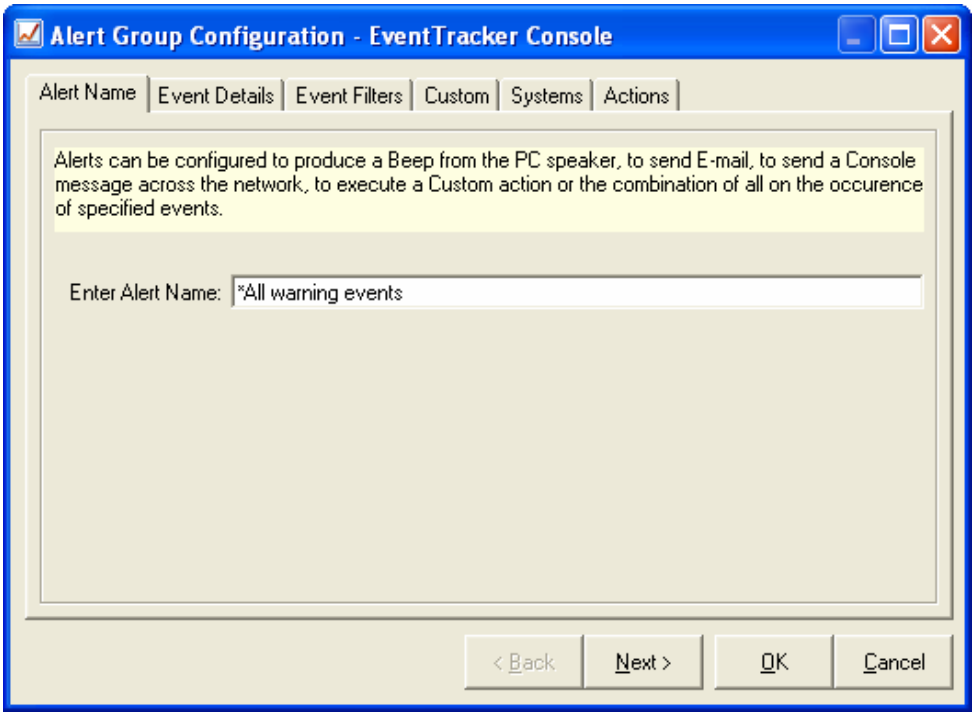
Right-click the Category that you want to configure as Alert.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Add As Alert**

EventTracker displays the Alert Group Configuration console.

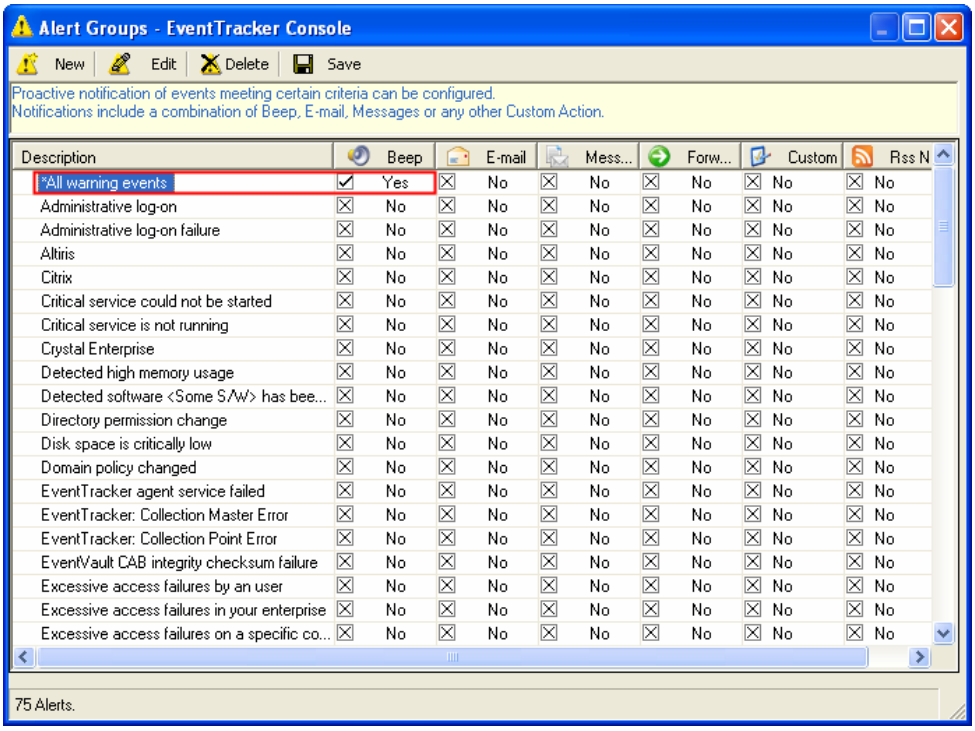
Figure 354 Alert Group Configuration Console


Alert Group Configuration - EventTracker Console
Alert Name
Event Details
Event Filters
Custom
Systems
Actions
Alerts can be configured to produce a Beep from the PC speaker, to send E-mail, to send a Console message across the network, to execute a Custom action or the combination of all on the occurence of specified events.
Enter Alert Name:
*All warning events
< Back
Next >
OK
Cancel

3. Type / select appropriately in the relevant tabs.
4. Click **OK**.
5. Open the Management Console.
6. Click the **Configure** menu and select the **Configure Alerts** option.

   EventTracker displays the Alert Groups console with the newly added Alert.

Figure 355 Alert Groups Console



Chapter 13
Export Import Utility

In this chapter, you will learn about:

- Export/Import Utility

Export and Import Utility

Export and Import Utility enables you to export/import custom Categories, Filters, Alerts, Schedule Reports, Domains, Systems and RSS Feeds during migrate/upgrade process, and to transfer EventTracker data from one system to the other in your enterprise. Suppose, you have configured Schedule Reports in System A and want to configure Schedule Reports in System B with same configuration settings. You need not configure again in System B, just export the Schedule Reports configured in System A and then import those .iscat files into System B.

Exporting Categories

To export Categories

1. Open the Management console.
2. Click the **Tools** menu and select the **Import and Export Utility** option

   (OR)

   Double-click Maintenance Tools on the Control Panel.

   Double-click Import and Export Utility.

   EventTracker displays the Export Import Utility.

Figure 356 Export Import Utility window – Export Category

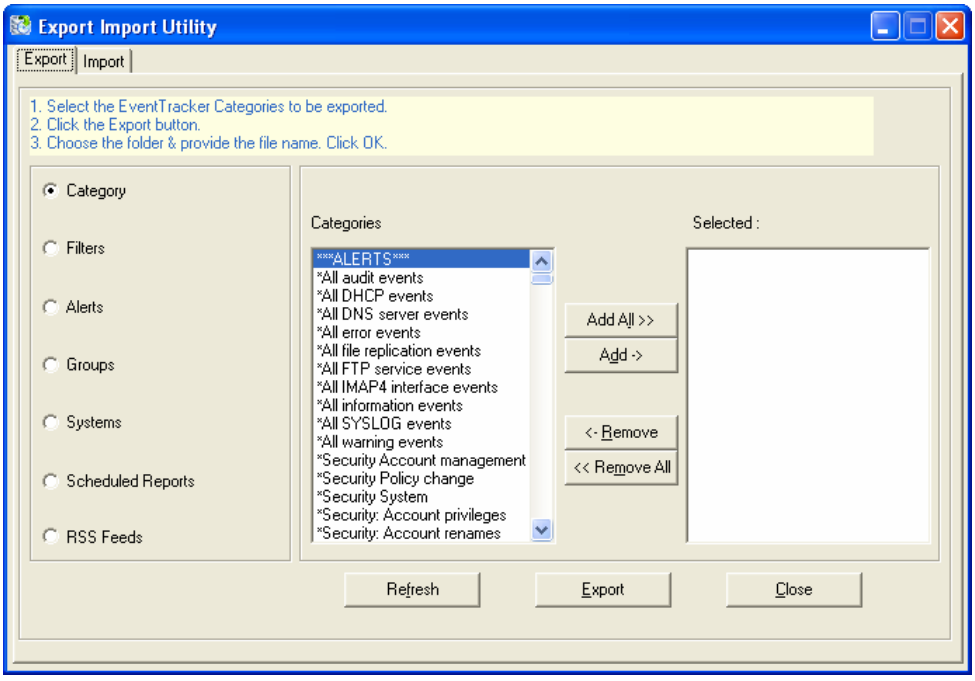


Table 67

Field	Description
Categories	Select a Category / Categories from this list. Click **Add->** to add the selected Category/Categories to the **Selected** list. Click **Add All>>** to export all the Categories. All the Categories are added to the Selected list.
Selected	Select a Category / Categories from this list. Click **<-Remove** to remove the selected Category/Categories from this list. Click **<<Remove All** to remove all the Categories from this list.
Refresh	Click to update the Categories.

3 Type appropriately in the relevant fields.

4 Click **Export**.

EventTracker displays the Select Export File dialog box.

5 Click the **Save in** drop-down box and select the path where you want to export the category.

6 Type the file name in the **File name** field.

> **Note**
>
> The valid file extension is `.iscat`.

7 Click **Save**.

EventTracker displays the Export Import Utility message box.

Figure 357 Export Category - message box

8 Click **OK**.

Exporting Filters

To export Filters

1. Open the Export Import Utility.
2. Select the **Filters** option.

   EventTracker displays the Export Import Utility.
3. Click **Export**.

   EventTracker displays the Select Export File dialog box.
4. Click the **Save in** drop-down box and select the path where you want to export the filters.
5. Enter the file name in the **File name** field.

> **Note**
>
> The valid file extension is `.isfil`.

6. Click **Save**.

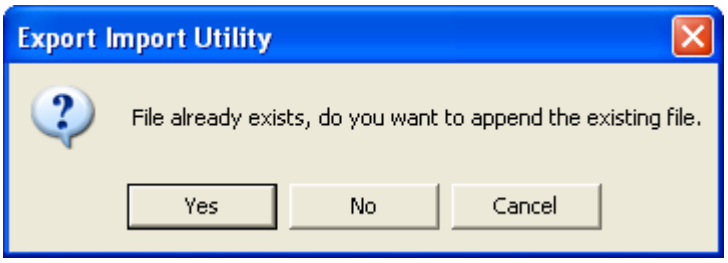
   EventTracker displays the Export Import Utility message box.

Figure 358 Export Filters - message box

7. Click **OK**.

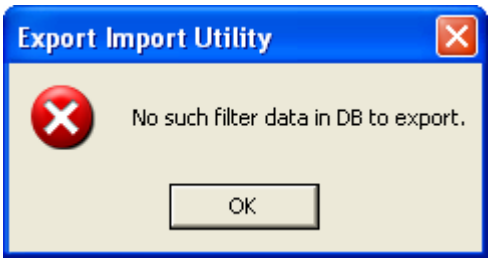
   If the file already exists, EventTracker displays the Export Import Utility message box.

Figure 359 Export Filters - message box



EventTracker displays Export Import Utility message box there is no filter detail exists in the database.

Figure 360 Export Filters - message box



Exporting Alerts

To export Alerts

1. Open the Export Import Utility.
2. Select the **Alerts** option.

   EventTracker displays the Export Import Utility.

Figure 361 Export Import Utility window – Export Alerts

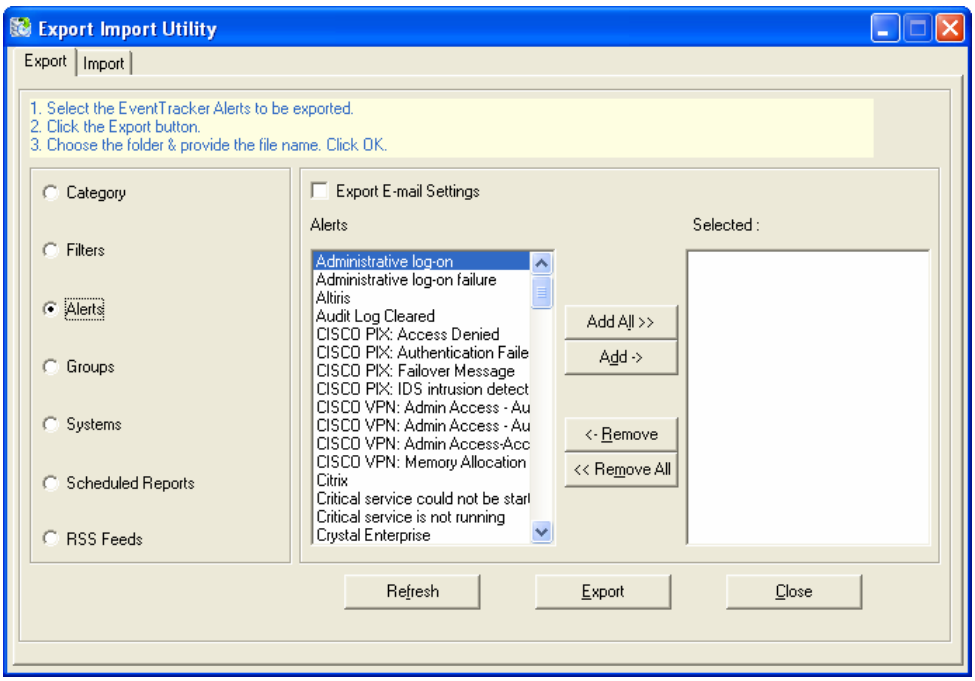


Table 68

Field	Description
Export Email Settings	Select this check box to export alerts with their e-mail settings if any.
Alerts	Select an Alert / Alerts from this list. Click **Add->** to add the selected Alert/Alerts to the **Selected** list. Click **Add All>>** to export all the Alerts. All the Alerts are added to the Selected list.
Export E-mail Settings	Select this check box to export e-mail configurations you have set, along with the Alerts.
Selected	Select an Alert / Alerts from this list. Click **<-Remove** to remove the selected Alert/Alerts from this list. Click **<<Remove All** to remove all Alerts from this list.
Refresh	Click to update the Alerts.

3 Type appropriately in the relevant fields.

4 Click **Export**.

EventTracker displays the Select Export File dialog box.

5 Click the **Save in** drop-down box and select the path where you want to export the alerts.

6 Enter the file name in the **File name** field.

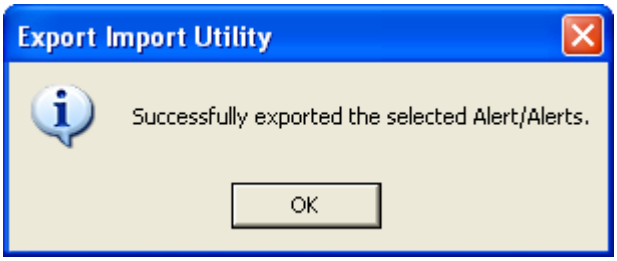
Note

The valid file extension is `.isalt`.

7 Click **Save**.

EventTracker displays the Export Import Utility message box.

Figure 362 Export Alerts - message box



8 Click **OK**.

Exporting System Groups

To export system groups

1. Open the Export Import Utility.
2. Select the **Groups** option.

   EventTracker displays the Export Import Utility.

Figure 363 Export Import Utility window – Export Domains

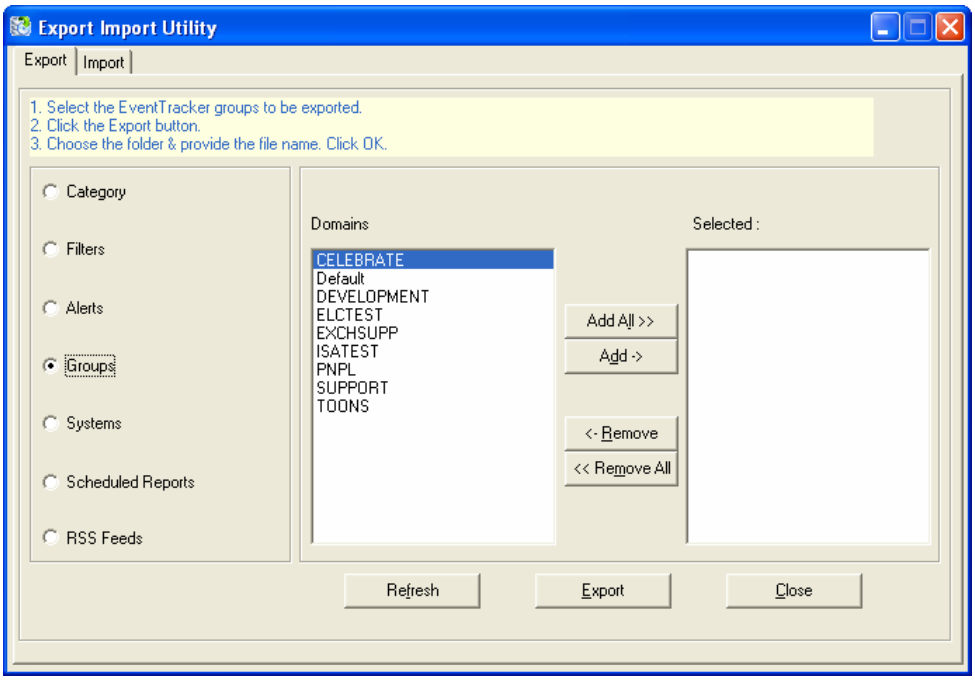


Table 69

Field	Description
Domains	Select a Domain / Domains from this list. Click **Add->** to add the selected Domain/Domains to the **Selected** list. Click **Add All>>** to export all the Domains. All the Domains are added to the Selected list.
Selected	Select a Domain / Domains from this list. Click **<-Remove** to remove the selected Domain/Domains from this list. Click **<<Remove All** to remove all the Domains from this list.
Refresh	Click to update the Domains.

3. Type appropriately in the relevant fields.
4. Click **Export**.

EventTracker displays the Select Export File dialog box.

5 Click the **Save in** drop-down box and select the path where you want to export the domains.

6 Type the file name in the **File name** field.

> **Note**
>
> The valid file extension is `.issys`.

7 Click **Save**.

EventTracker displays the Export Import Utility message box.

Figure 364 Export Domains - message box

8 Click **OK**.

Exporting Systems

To export systems

1 Open the Export Import Utility.

2 Select the **Systems** option.

EventTracker displays the Export Import Utility.

Figure 365 Export Import Utility window – Export Systems

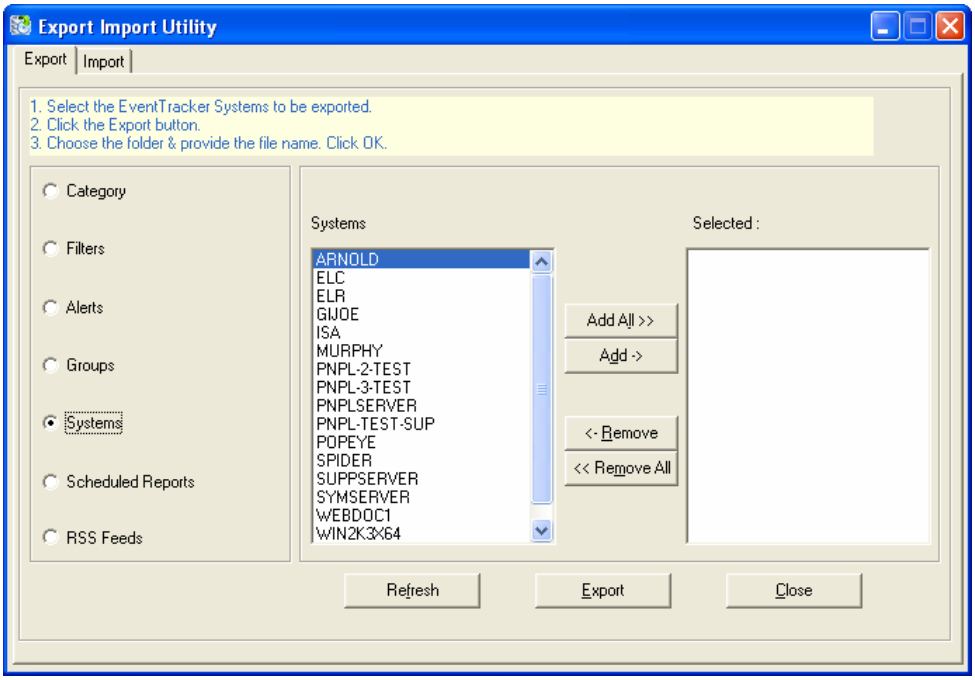


Table 70

Field	Description
Systems	Select a System / Systems from this list. Click **Add->** to add the selected System/Systems to the **Selected** list. Click **Add All>>** to export all the Systems. All the Systems are added to the Selected list.
Selected	Select a System / Systems from this list. Click **<-Remove** to remove the selected System/Systems from this list. Click **<<Remove All** to remove all the Systems from this list.
Refresh	Click to update the Systems.

3. Type appropriately in the relevant fields.
4. Click **Export**.

   EventTracker displays the Select Export File dialog box.
5. Click the **Save in** drop-down box and select the path where you want to export the systems.
6. Type the file name in the **File name** field.

Note

The valid file extension is `.issys`.

7 Click **Save**.

EventTracker displays the Export Import Utility message box.

Figure 366 Export Systems - message box

8 Click **OK**.

Exporting Schedule Reports

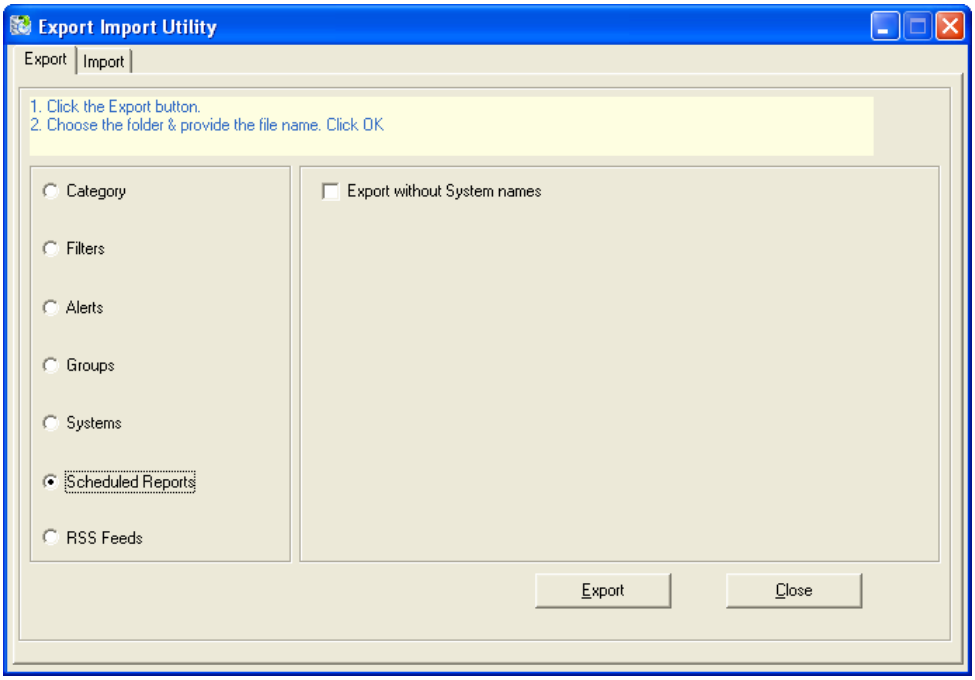
To export Scheduled Reports

1 Open the Export Import Utility.

2 Select the **Scheduled Reports** option to export Advanced Reports Console Scheduled Reports.

EventTracker displays the Export Import Utility.

Figure 367 Export Import Utility window – Export Scheduled Reports



3. Select the **Export without System names** check box to export the schedule configuration without system names. Exporting schedule configurations without the system names helps to apply the settings to any environment. If exported with system names and the systems do not exist in the target environment, then the scheduled reports fail.
4. Click **Export**.

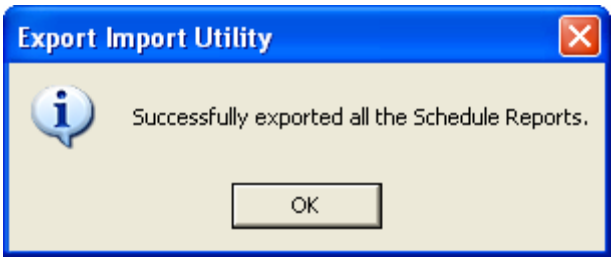
   EventTracker displays the Select Export File dialog box.
5. Click the **Save in** drop-down box and select the path where you want to export the filters.
6. Type the file name in the **File name** field.

> **Note**
>
> The valid file extension is `.issch`.

7. Click **Save**.

   EventTracker displays the Export Import Utility message box.

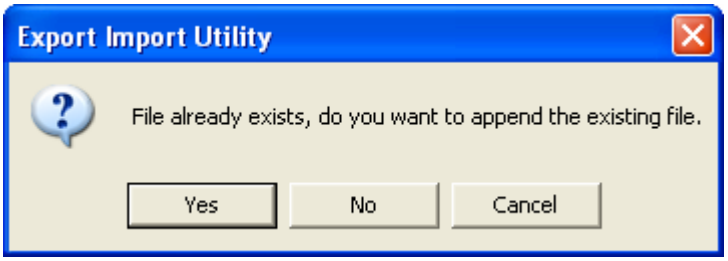
Figure 368 Export Scheduled Reports - message box



8 Click **OK**.

If the file already exists, EventTracker displays the Export Import Utility message box.

Figure 369 Export Filters - message box



Exporting RSS Feeds

To export RSS Feeds

1 Open the Export Import Utility.

2 Select the **RSS Feeds** option.

EventTracker displays the Export Import Utility.

3 Click **Export**.

EventTracker displays the Select Export File dialog box.

4 Click the **Save in** drop-down box and select the path where you want to export the filters.

5 Type the file name in the **File name** field.

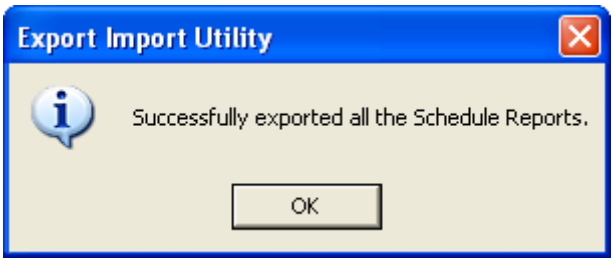
Note

The valid file extension is `.issrss`.

6 Click **Save**.

EventTracker displays the Export Import Utility message box.

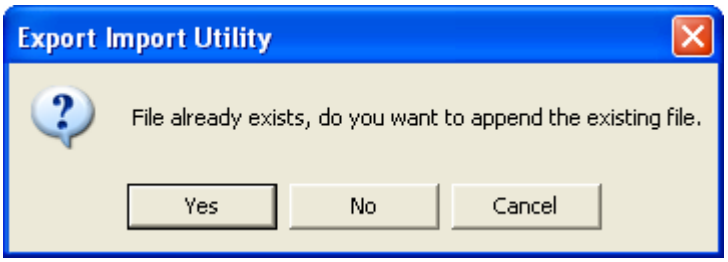
Figure 370 Export Scheduled Reports - message box



7 Click **OK**.

If the file already exists, EventTracker displays the Export Import Utility message box.

Figure 371 Export Filters - message box



Importing Categories

To import Categories

1 Open the Management Console.

2 Click the **Tools** menu and select the **Import and Export Utility** option.

(OR)

Double-click Maintenance Tools on the Control Panel.

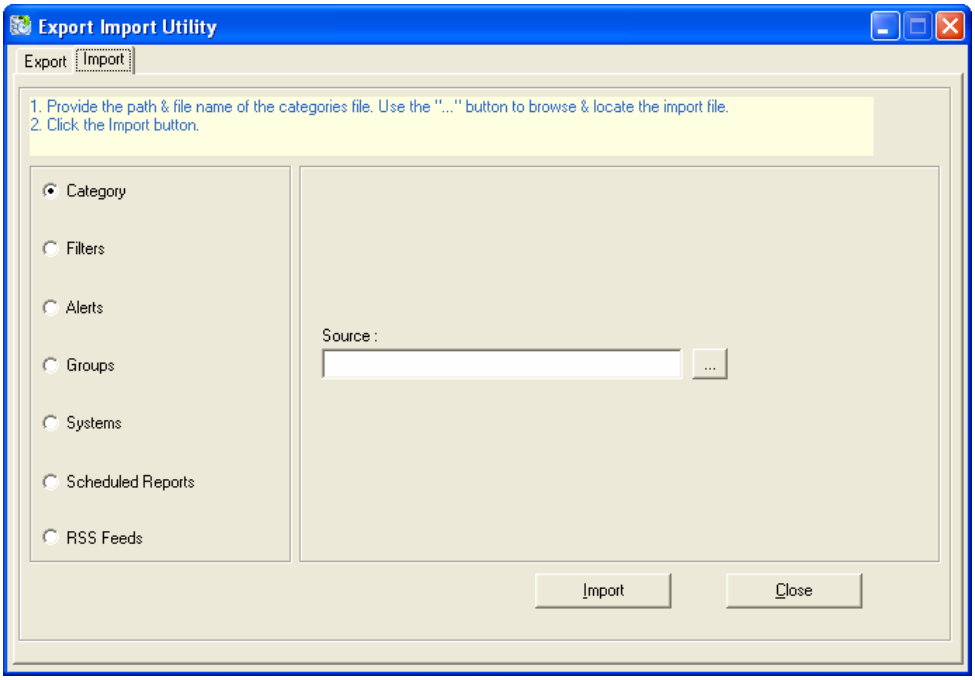
Double-click Import and Export Utility.

EventTracker displays the Export Import Utility.

3 Click the **Import** tab.

EventTracker displays the Export Import Utility.

Figure 372 Export Import Utility window – Import tab



4 **Category** option is selected by default.

5 Click ... located adjacent to the **Source** field.

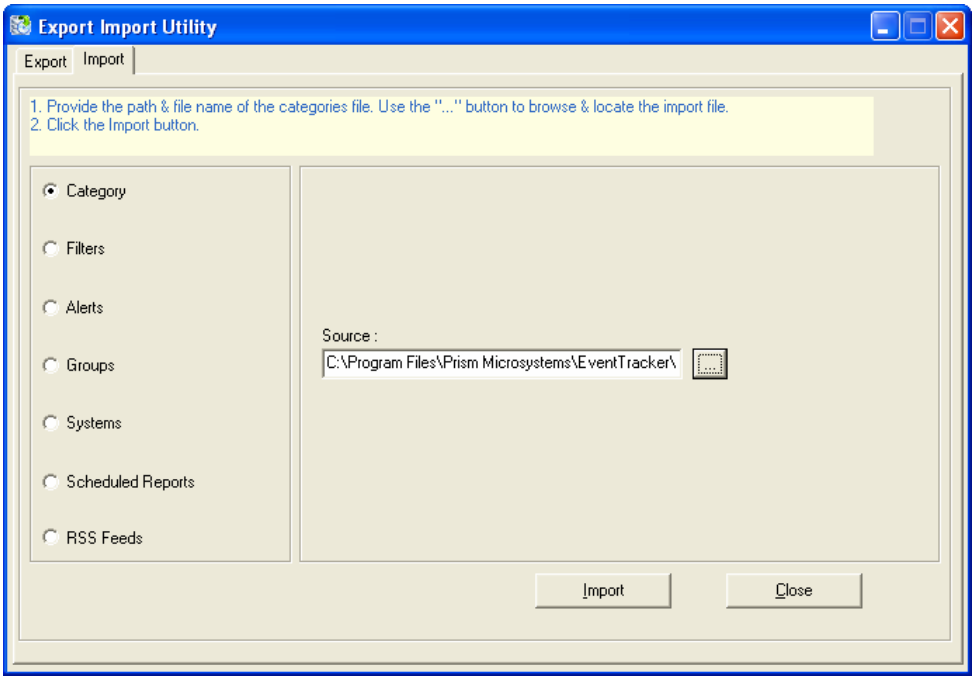
EventTracker displays the Select *.iscat File dialog box.

6 Navigate and locate the category file you want to import.

7 Click **Open**.

EventTracker displays the Import tab on the Export Import Utility.

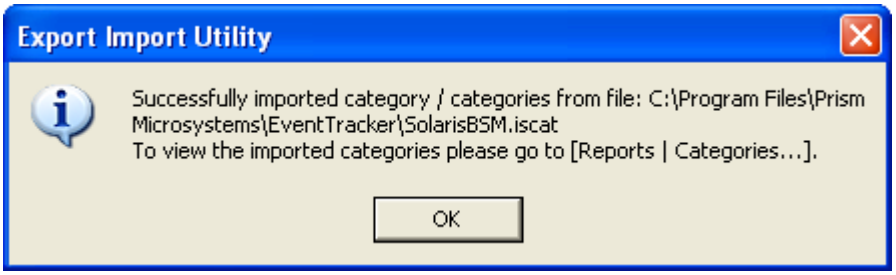
Figure 373 Export Import Utility window – Import Category



8 Click **Import**.

EventTracker displays the Export Import Utility message box.

Figure 374 Import Category - message box


Export Import Utility
Successfully imported category / categories from file: C:\Program Files\Prism Microsystems\EventTracker\SolarisBSM.iscat
To view the imported categories please go to [Reports | Categories...].
OK

9 Click **OK**.

Importing Filters

To import Filters

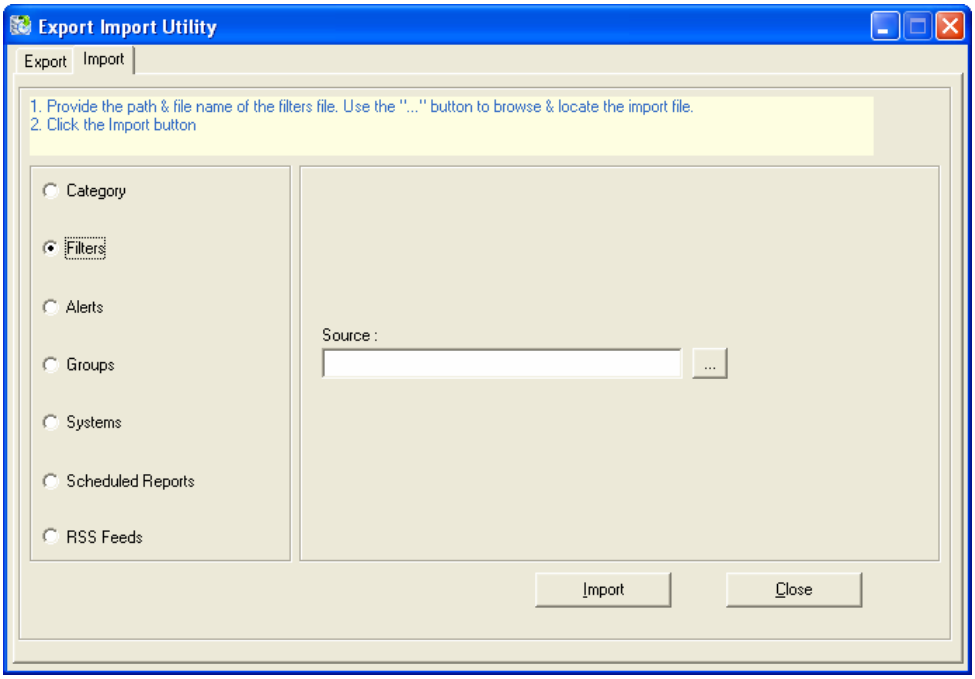
1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **Filters** option on the **Import** tab.

EventTracker displays the Export Import Utility.

Figure 375 Export Import Utility window – Import Filters



4 Click ... located adjacent to the **Source** field.

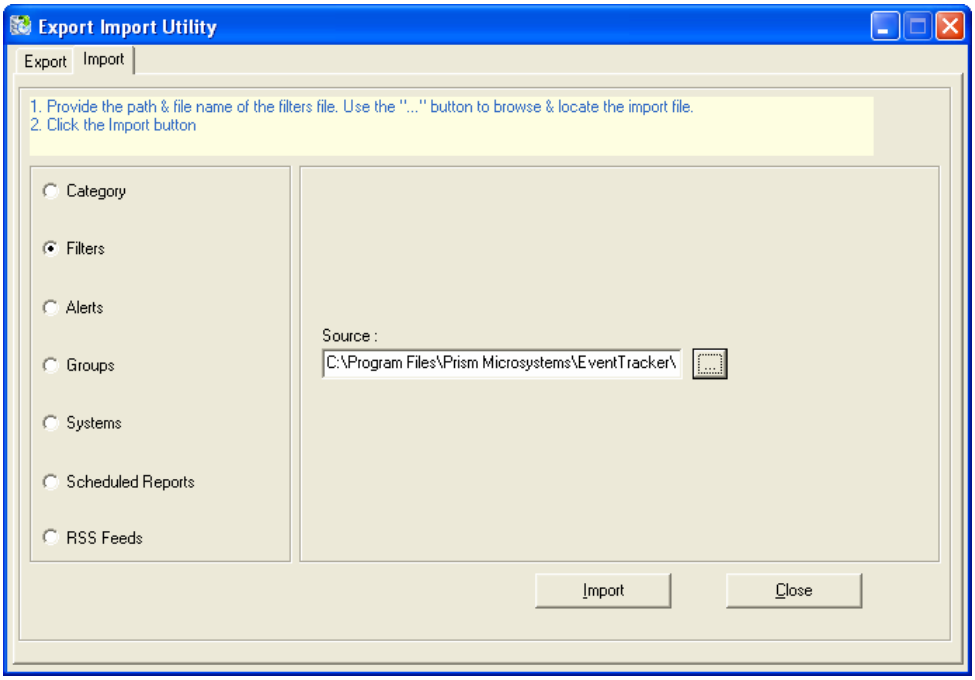
EventTracker displays the Select *.isfil File dialog box.

5 Navigate and locate the filters file you want to import.

6 Click **Open**.

EventTracker displays the Import tab on the Export Import Utility.

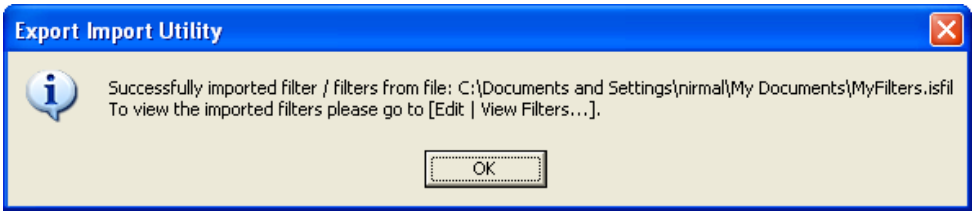
Figure 376 Export Import Utility window – Import Filters



7 Click **Import**.

EventTracker displays the Export Import Utility message box.

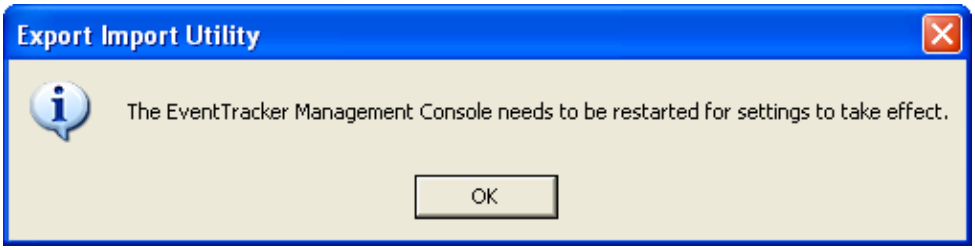
Figure 377 Import Filters- message box


Export Import Utility
Successfully imported filter / filters from file: C:\Documents and Settings\nirmal\My Documents\MyFilters.isfil
To view the imported filters please go to [Edit | View Filters...].
OK

8 Click **OK**.

EventTracker displays the Export Import Utility message box.

Figure 378 Import Filters- message box



9 Click **OK** and restart the Management Console.

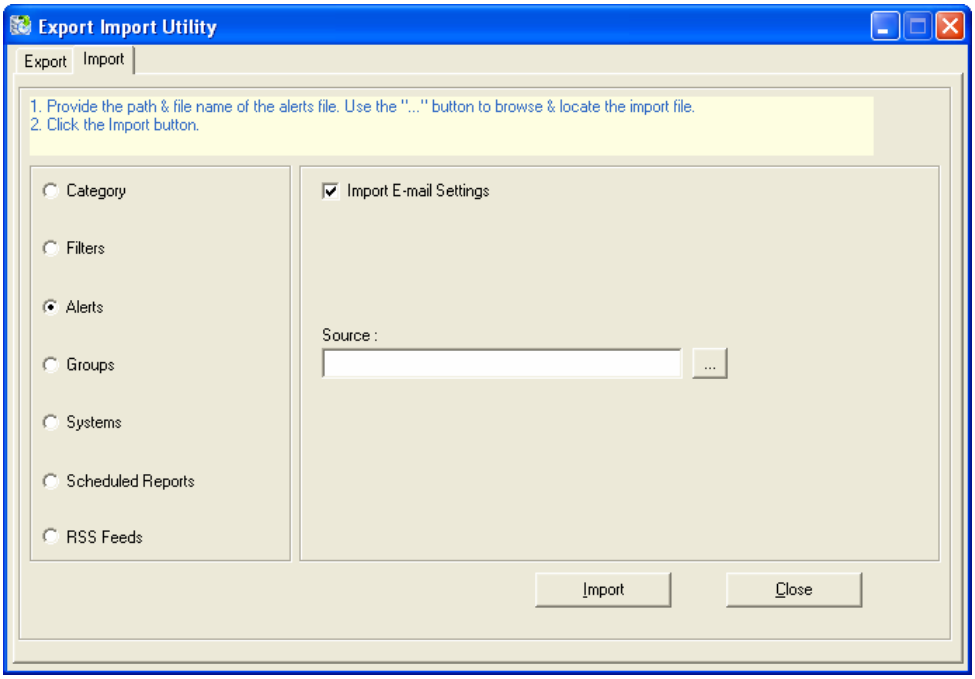
Importing Alerts

To import Alerts

1. Open the Export Import Utility.
2. Click the **Import** tab.
3. Select the **Alerts** option on the **Import** tab.

   EventTracker displays the Export Import Utility.

Figure 379 Export Import Utility window – Import Alerts

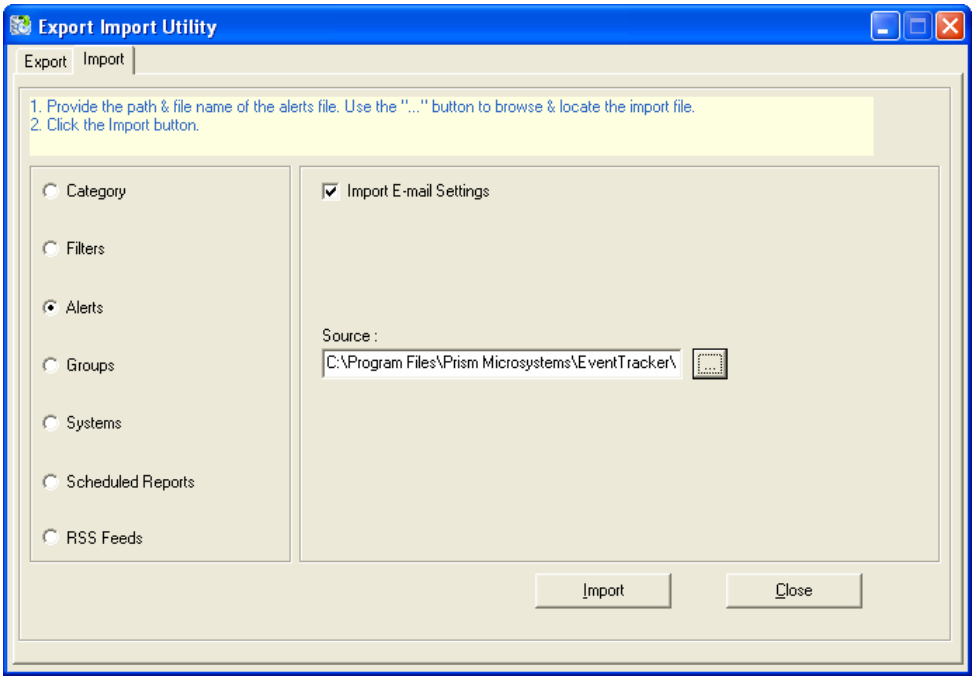


4. Click ... located adjacent to the **Source** field.

   EventTracker displays the Select *.isalt File dialog box.
5. Navigate and locate the Alerts file you want to import.
6. Click **Open**.

   EventTracker displays the Import tab on the Export Import Utility.

Figure 380 Export Import Utility window – Import Alerts

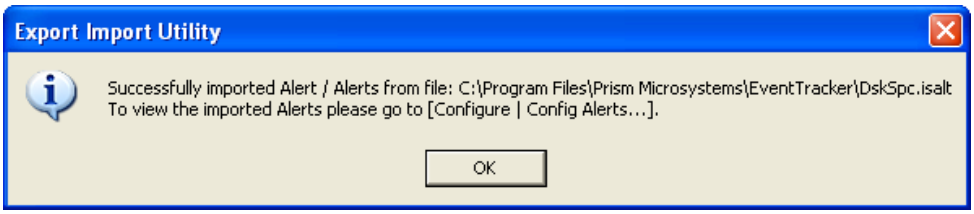


7 **Import E-mail Settings** check box is selected by default to import the Alerts with their e-mail configuration settings. Clear this check box to import Alerts without their e-mail settings.

8 Click **Import**.

EventTracker displays the Export Import Utility message box.

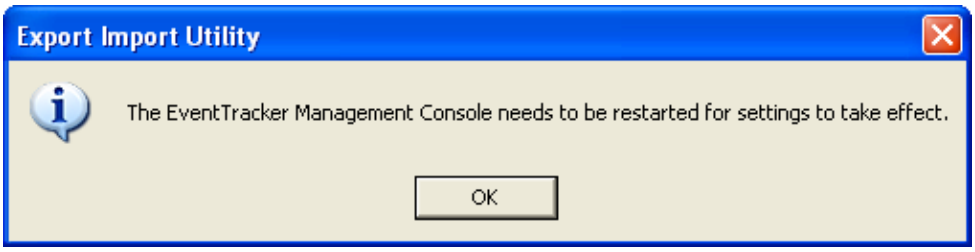
Figure 381 Import Alerts - message box


Export Import Utility
Successfully imported Alert / Alerts from file: C:\Program Files\Prism Microsystems\EventTracker\DskSpc.isalt
To view the imported Alerts please go to [Configure | Config Alerts...].
OK

9 Click **OK**.

EventTracker displays the Export Import Utility message box.

Figure 382 Import Alerts - message box



EventTracker displays the Export Import Utility message box if the alerts already do exist.

Figure 383 Import Alerts - message box

Export Import Utility
Current file contains multiple Alerts and some or all of the Alerts were already existing. These Alerts were automatically updated. The rest were imported successfully.
OK

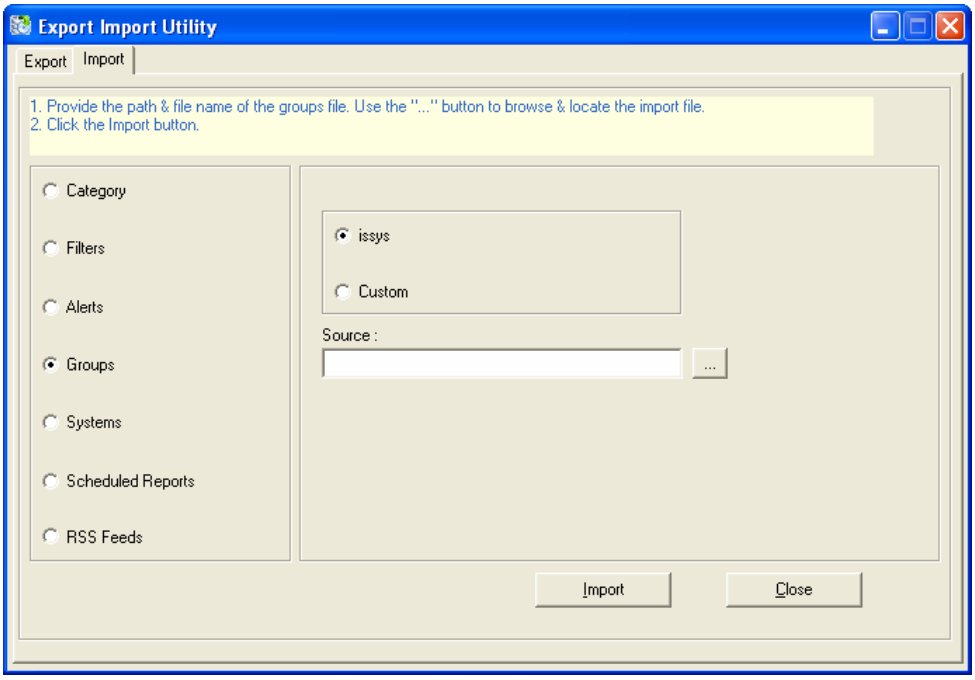
Importing System Groups

To import system groups

1. Open the Export Import Utility.
2. Click the **Import** tab.
3. Select the **Groups** option on the **Import** tab.

   EventTracker displays the Export Import Utility.

Figure 384 Export Import Utility window – Import Domains



4. Select the **issys** option to import the `issys` type file.

   (OR)

Select the **Custom** option to import other type of files such as `txt` files.

5 Click ... located adjacent to the **Source** field.

EventTracker displays the Select *.issys File dialog box, if you select the **issys** option.

6 Navigate and locate the domains file you want to import and click **Open**.

Note

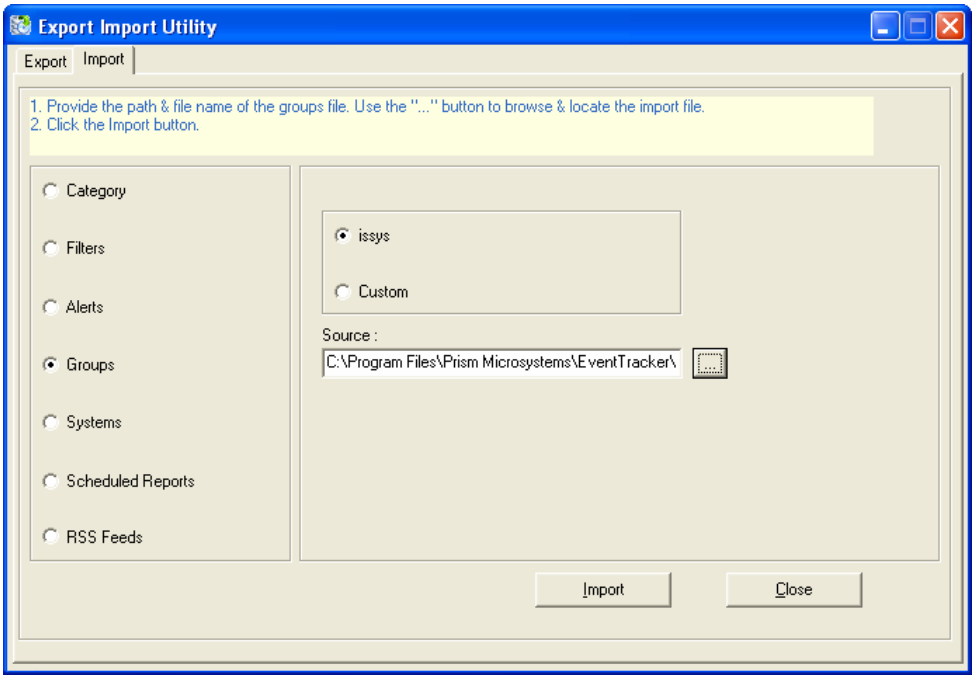
The valid file extension is `.issys`.

EventTracker displays the Select *.* File dialog box, if you select the **Custom** option.

7 Navigate and locate the domains file you want to import and click **Open**.

EventTracker displays the Import tab on the Export Import Utility.

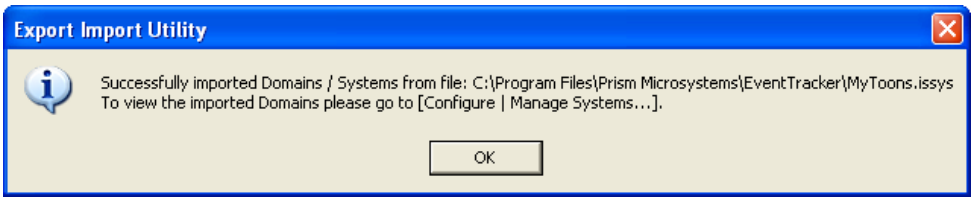
Figure 385 Export Import Utility window – Import Domains



8 Click **Import**.

EventTracker displays the Export Import Utility message box.

Figure 386 Import Domains - message box


Export Import Utility
Successfully imported Domains / Systems from file: C:\Program Files\Prism Microsystems\EventTracker\MyToons.issys
To view the imported Domains please go to [Configure | Manage Systems...].
OK

9 Click **OK**.

Importing Systems

To import Systems

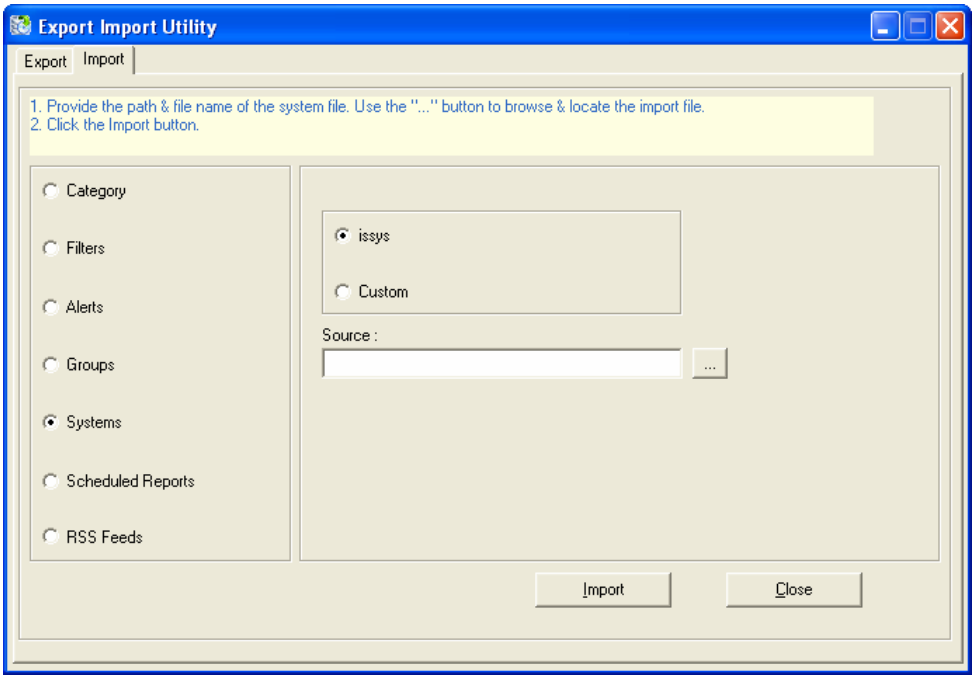
1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **Systems** option on the **Import** tab.

EventTracker displays the Export Import Utility.

Figure 387 Export Import Utility window – Import Systems



4 Select the **issys** option to import the `issys` type file.

(OR)

Select the **Custom** option to import other type of files such as `txt` files.

5 Click ... located adjacent to the **Source** field.

EventTracker displays the Select *.issys File dialog box, if you select the **issys** option.

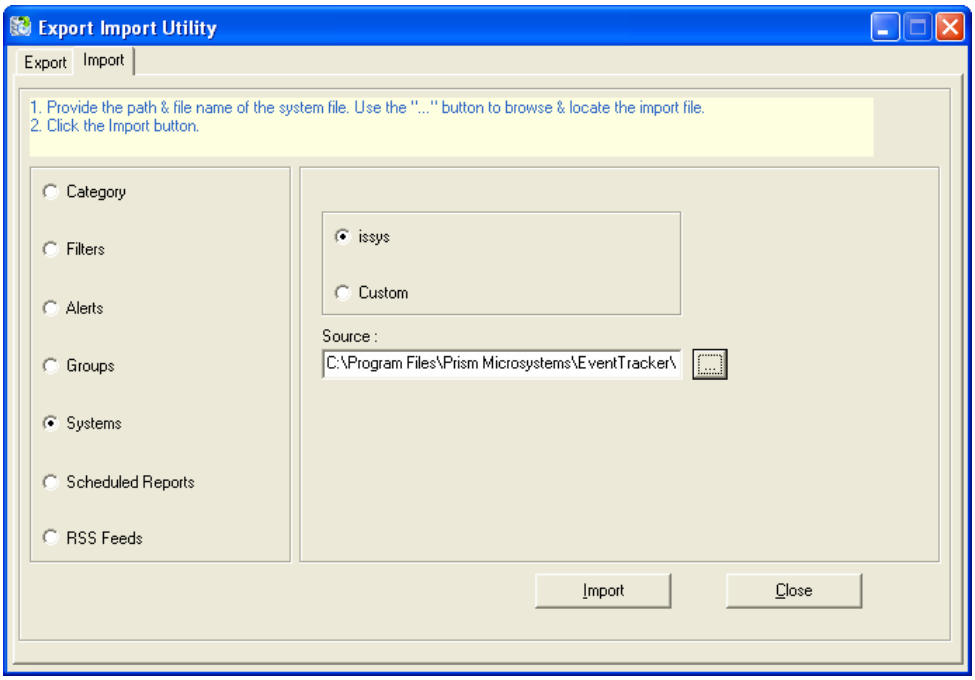
6 Navigate and locate the systems file you want to import and click **Open**.

EventTracker displays the Select *.* File dialog box, if you select the **Custom** option.

7 Navigate and locate the systems file you want to import and click **Open**.

EventTracker displays the Import tab on the Export Import Utility dialog box.

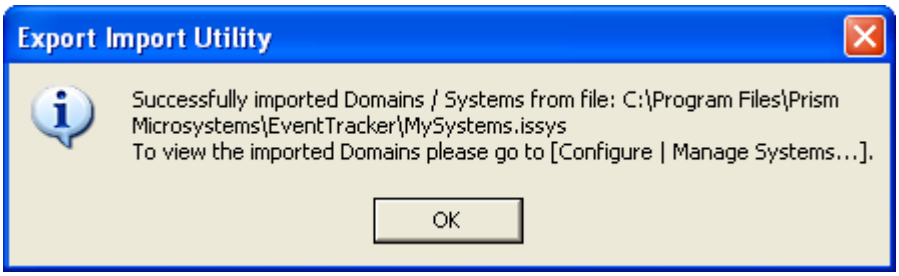
Figure 388 Export Import Utility window – Import Systems



8 Click **Import**.

EventTracker displays the Export Import Utility message box.

Figure 389 Import Systems - message box


Export Import Utility
Successfully imported Domains / Systems from file: C:\Program Files\Prism Microsystems\EventTracker\MySystems.issys
To view the imported Domains please go to [Configure | Manage Systems...].
OK

9 Click **OK**.

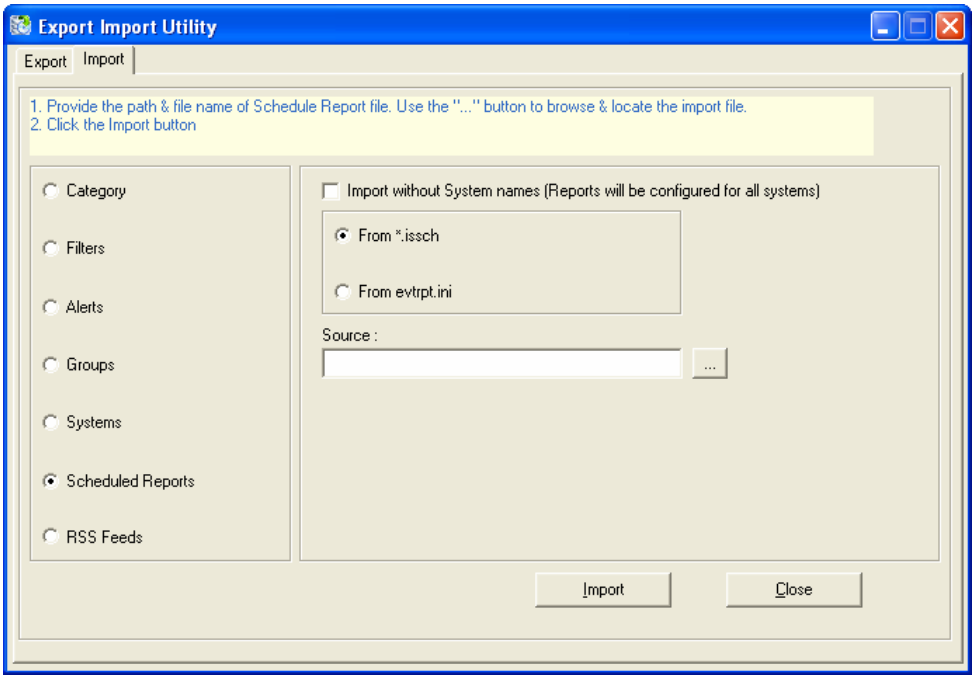
Importing Schedule Reports

To import Schedule Reports

1. Open the Export Import Utility.
2. Click the **Import** tab.
3. Select the **Scheduled Reports** option to import new Reports Console Scheduled Reports.

   EventTracker displays the Export Import Utility.

Figure 390 Export Import Utility window – Import Scheduled Reports



4. Select the **Import without System names** check box to import the configuration settings without system names. The settings will be applied to all systems in the target environment.
5. Select the **issch** option to import the `issch` type files.

   (OR)

   Select the **Custom** option to import `evtrpt.ini` file.
6. Click ... located adjacent to the **Source** field.

   EventTracker displays the Select *.issch File dialog box, if you select the **issch** option.

7 Navigate and locate the scheduled reports file you want to import and click **Open**.

EventTracker displays the Select evtrpt.ini File dialog box, if you select the evtrpt.ini option.

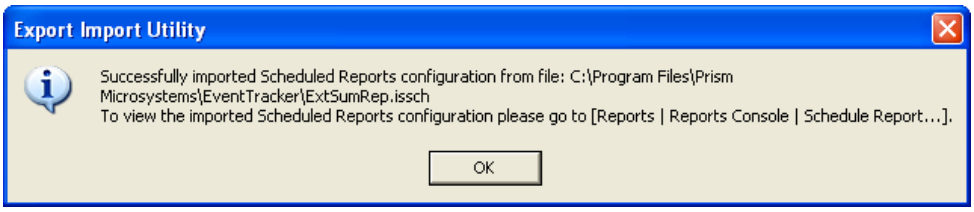
8 Navigate and locate the systems file you want to import and click **Open**.

EventTracker displays the Import tab on the Export Import Utility dialog box.

9 Click **Import**.

EventTracker displays the Export Import Utility message box.

Figure 391 Import Systems - message box


Export Import Utility
Successfully imported Scheduled Reports configuration from file: C:\Program Files\Prism Microsystems\EventTracker\ExtSumRep.issch
To view the imported Scheduled Reports configuration please go to [Reports | Reports Console | Schedule Report...].
OK

10 Click **OK**.

Importing RSS Feeds

To import RSS Feeds

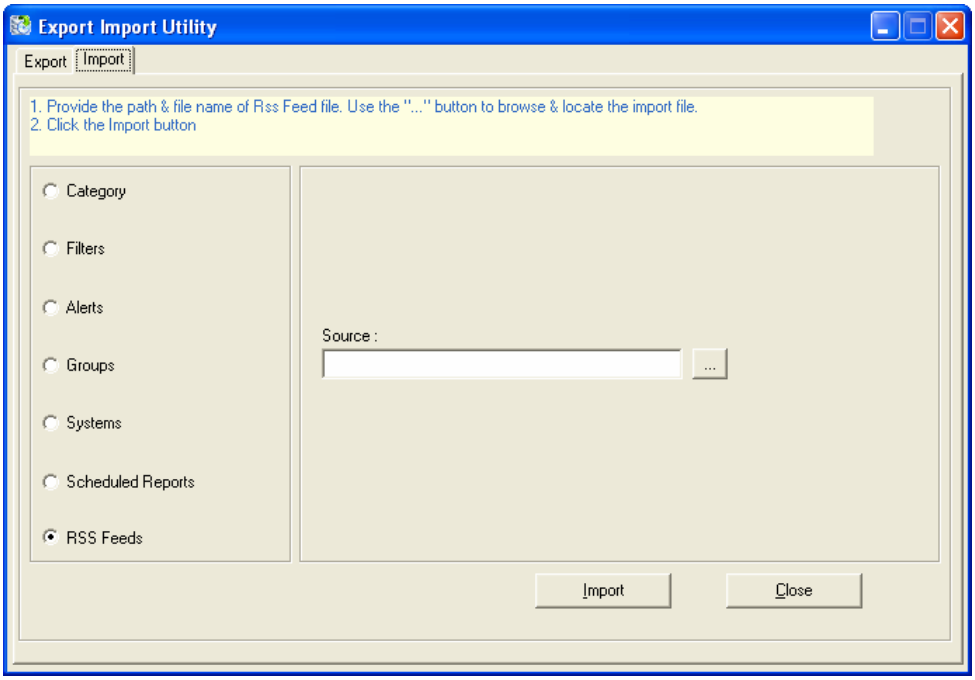
1 Open the Export Import Utility.

2 Click the **Import** tab.

3 Select the **RSS Feeds**.

EventTracker displays the Export Import Utility.

Figure 392 Export Import Utility window – Import Scheduled Reports



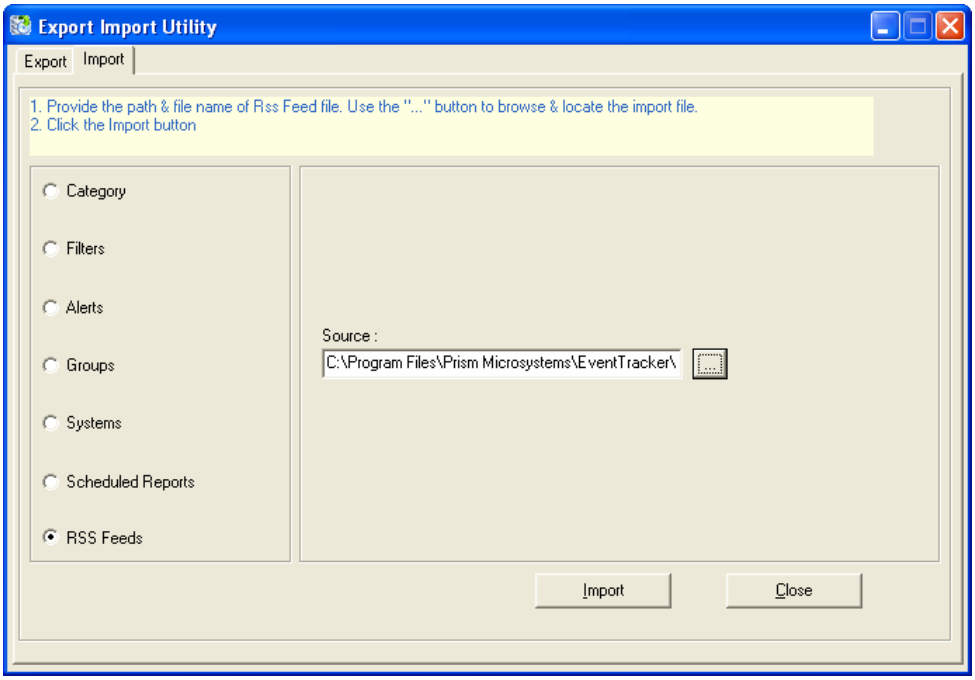
4 Click ... located adjacent to the **Source** field.

EventTracker displays the Select *.issrss File dialog box.

5 Navigate and locate the scheduled reports file you want to import and click **Open**.

6 EventTracker displays the Import tab on the Export Import Utility.

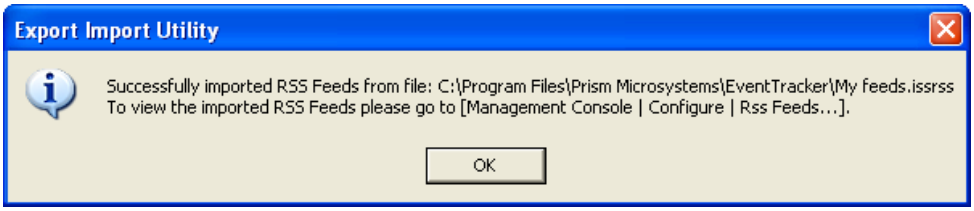
Figure 393 Export Import Utility window – Import Scheduled Reports



7 Click **Import**.

EventTracker displays the Export Import Utility message box.

Figure 394 Import Systems - message box


Export Import Utility
Successfully imported RSS Feeds from file: C:\Program Files\Prism Microsystems\EventTracker\My feeds.issrss
To view the imported RSS Feeds please go to [Management Console | Configure | Rss Feeds...].
OK

8 Click **OK**.

Chapter 14
Collection Point Model

In this chapter, you will learn about:

- Collection Point model
- Real World Scenarios

What is Collection Point model

As the volume of event logs and the complexity of corporate network infrastructure grow day-by-day at an unfathomable rate, mining the esoteric event log data becomes a taxing task for the network administrator. Prism recognized the gravity of the issue and came up with a holistic and single view management model, which is called Collection Point model. Collection Point model facilitates you to collect cab files from geographically or logically dispersed branch offices and generate consolidated audit reports from a centralized location. Collection Point works on a client-server model, whereby the Collection Points (clients) installed at the branch office locations periodically send the cab files to the Collection Master (server) installed at the corporate headquarters.

Since Collection Point model utilizes TCP as a transport layer, Collection Master (server) acknowledges every packet sent by Collection Points (clients). This assures recovery from data that is damaged, lost, duplicated, or delivered out of order by the Internet communication system. Moreover, the encryption mechanism assures the confidentiality and integrity of data is not compromised while it traverses through the public network. Every Collection Point (client) can be configured to report up to five Collection Masters (servers) simultaneously.

Standard Console

Best suited for (single-level) flat topologies where all monitored nodes report directly to one or more EventTracker Managers.

Collection Master Console

Best suited for hierarchical topologies. Being designated as a Collection Master, receives archives (CAB files) replicated by Collection Points.

Collection Point Console

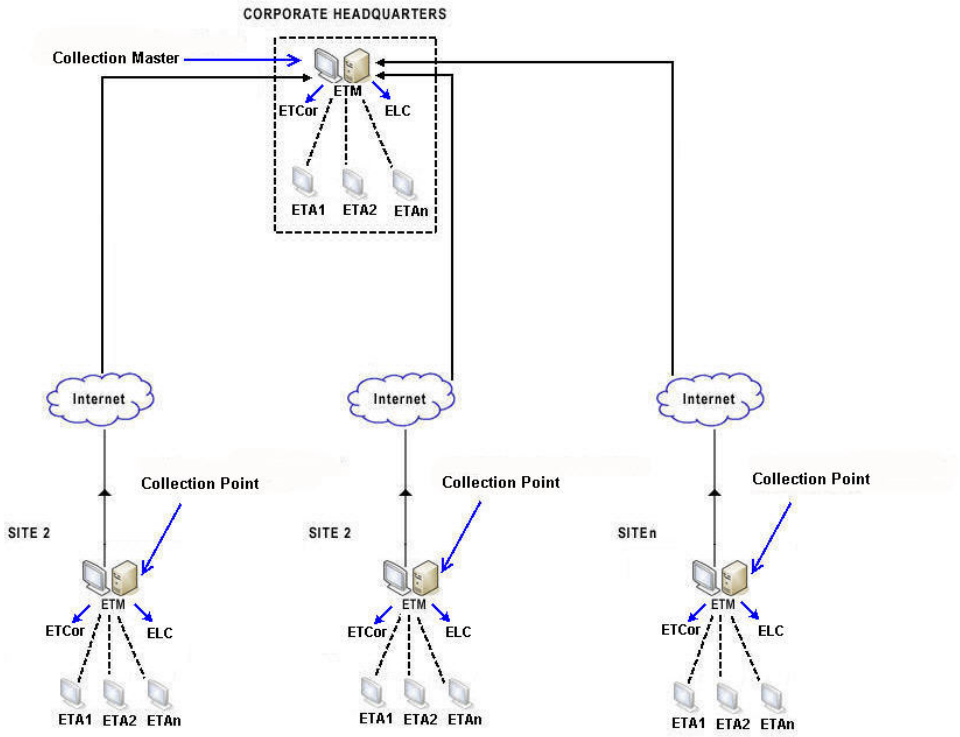
Best suited for hierarchical topologies where all monitored nodes report directly to a local EventTracker Manager, which is designated as a Collection Point, replicates archives (CAB files) to one or more Collection Masters.

Scalability

Collection Point model is best suited for organizations having multiple sites. The sites may geographically spread across the globe or do exist in the same precinct but with a robust setup

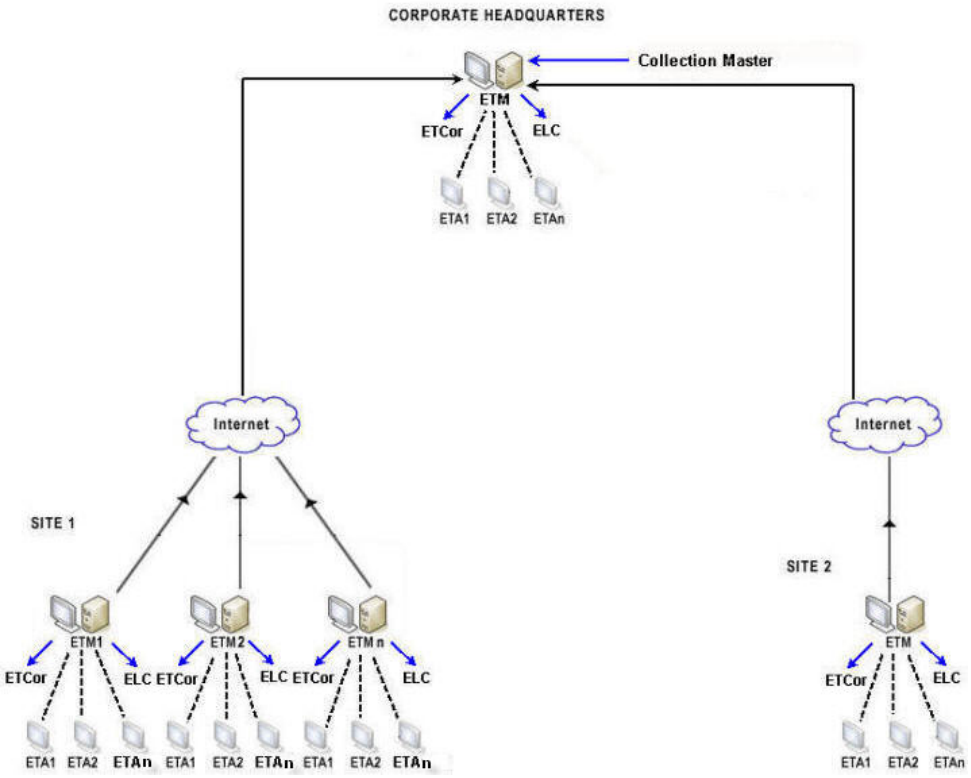
Real world scenarios

Figure 395 Scenario 1



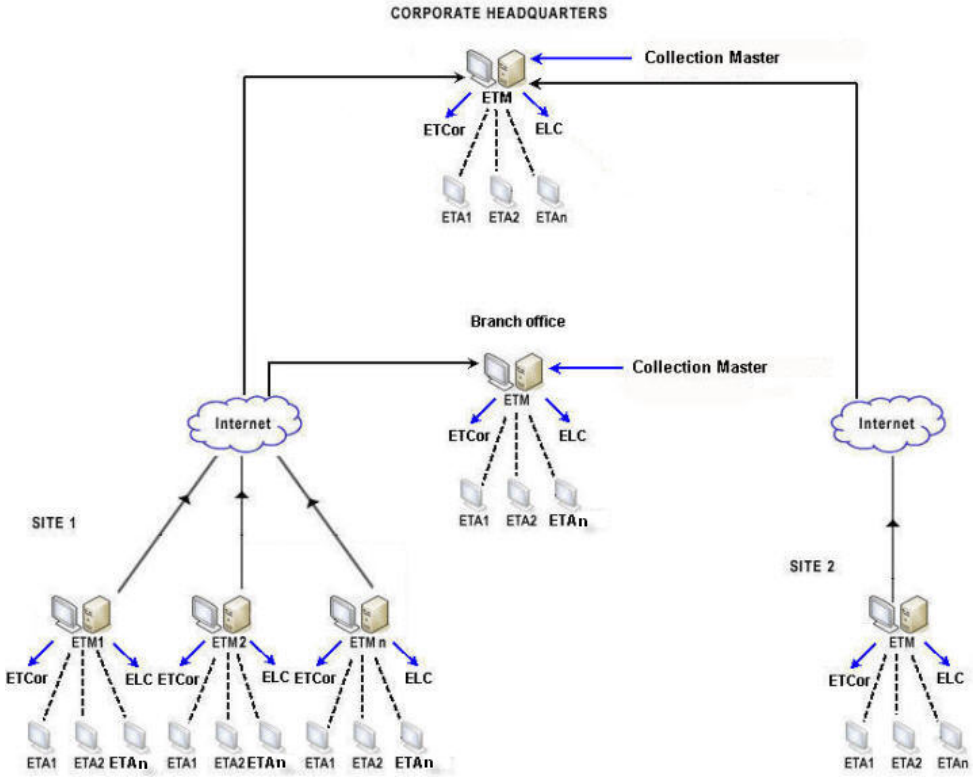
In the above-depicted scenario, all the Collection Points (clients) send their respective cab files periodically to the Collection Master (server) at the corporate headquarters.

Figure 396 Scenario 2



In this scenario, SITE 1 does exist physically in the same premises, which runs n number of EventTracker Managers. Each EventTracker Manager running Collection Point (client) will send the respective cab files to the Collection Master (server). The crux of the matter is that the Collection Master treats every individual EventTracker Manager running Collection Point (client) and the constellation of EventTracker Agents as different entities, no matter whether they exist in the same campus or on the same floor.

Figure 397 Scenario 3



The scenario above corroborates the statement that one Collection Point (client) could be configured to report up to five Collection Masters (servers).

Chapter 15
Collection Master

In this chapter, you will learn how to:

- Start Collection Master Console
- View Collection Point Details
- View CAB status
- Configure Collection Master listening port
- Merge Collection Points
- Request CAB files
- Delete CAB files
- Delete Collection Point Detail
- Configure Alerts

Starting Collection Master Console

This option helps you open Collection Master Console.

To open Collection Master Console

1 Open the EventTracker Control Panel.

2 Double-click

(OR)

Click Start, point to Programs, point to Prism Microsystems, point to EventTracker, and then select **EventTracker Collection Master Configuration** option.

EventTracker displays the Collection Master Console.

Figure 398 EventTracker Collection Master Console

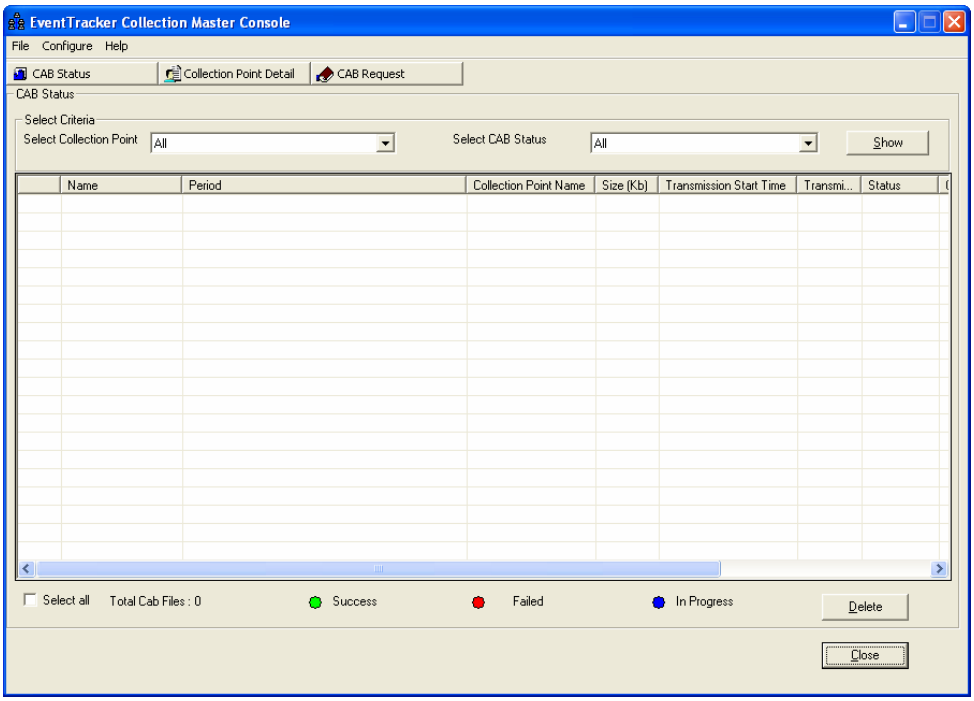


Table 71

Click	To
Collection Point Detail	View Collection Point details.
CAB Status	View status of CAB files received from Collection Points.
CAB Request	Send a request to a Collection Point to forward CAB files missing

Click	To
	in the source or CAB files that are failed to transfer.

Table 72

Field	Description
Select Criteria	
Select Collection Point	Select Collection Point from this drop-down list. All clients reporting to the Collection Master are listed in this drop-down list.
Select CAB Status	Select the status of the cab files from this drop-down list and then click **Show**. Available options are **All**, **Success**, **Failed** and **In Progress**.
Select all	Select this check box to mark all the CAB files for deletion and then click **Delete**. You can also select individual file for deletion.

Viewing Collection Point Details

This option helps you view details of the Collection Points that are forwarding CAB files to the Collection Master.

To view Collection Point Details

1. Click **Collection Point Detail** on the Collection Master Console.

   EventTracker displays the Collection Point Detail.

Figure 399 Collection Point Detail

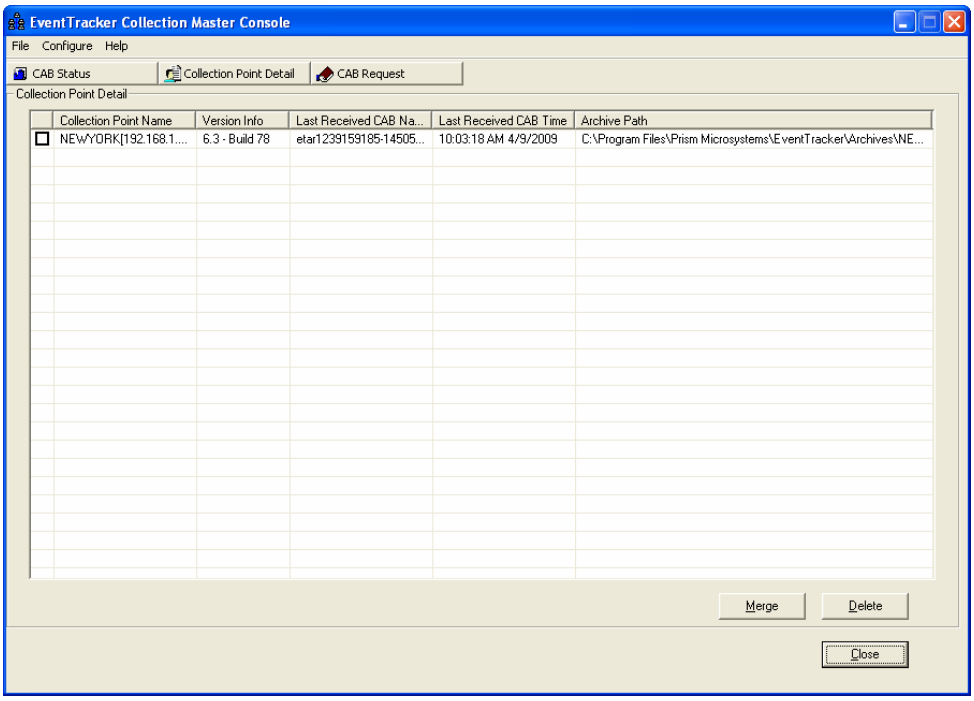


Table 73

Field	Description
Collection Point Name	Displays the name of the Collection Points that are reporting to the Collection Master.
Version Info	Displays the version of the Collection Points.
Last Received CAB Name	Name of the last CAB file that is received from Collection Points.
Last Received CAB Time	Date and Time when the Collection Master received the last CAB file.
Archive Path	Displays the path of the folder where cab files of the respective Collection Points are stored at the Collection Master computer. Example: …\Program Files\Prism Microsystems\EventTracker\Archives\NEWYORK[192.168.1.38]

Viewing CAB Status

This option helps you view status of the cab files transferred and being transferred by the Collection Points to the Collection Master.

To view CAB status

1 Click **CAB Status** on the Collection Master Console.

EventTracker displays the CAB Status.

Figure 400 CAB Status

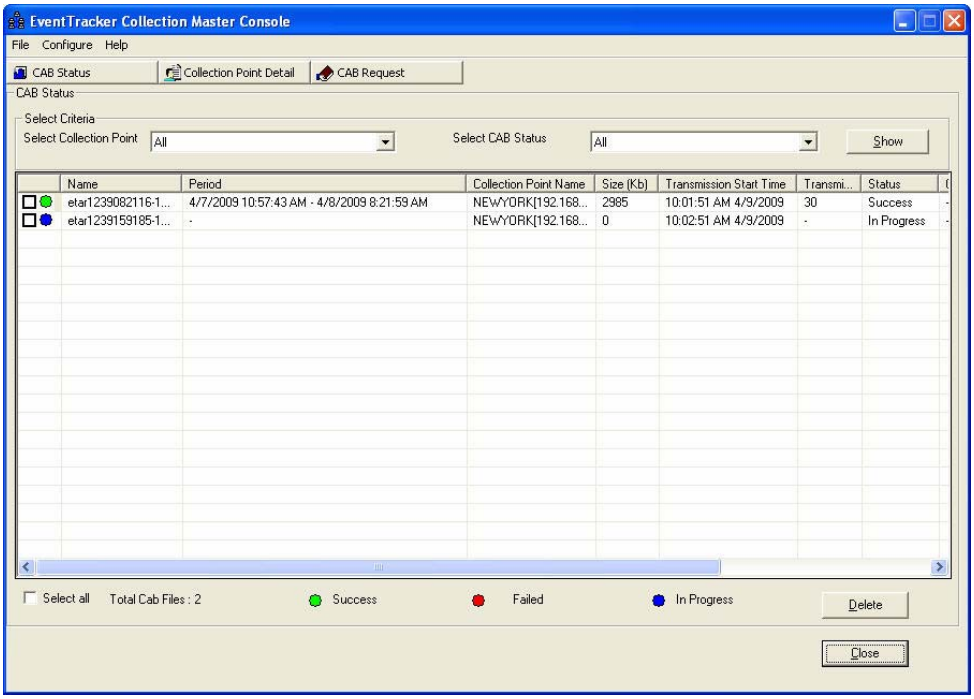


Figure 401 CAB Status

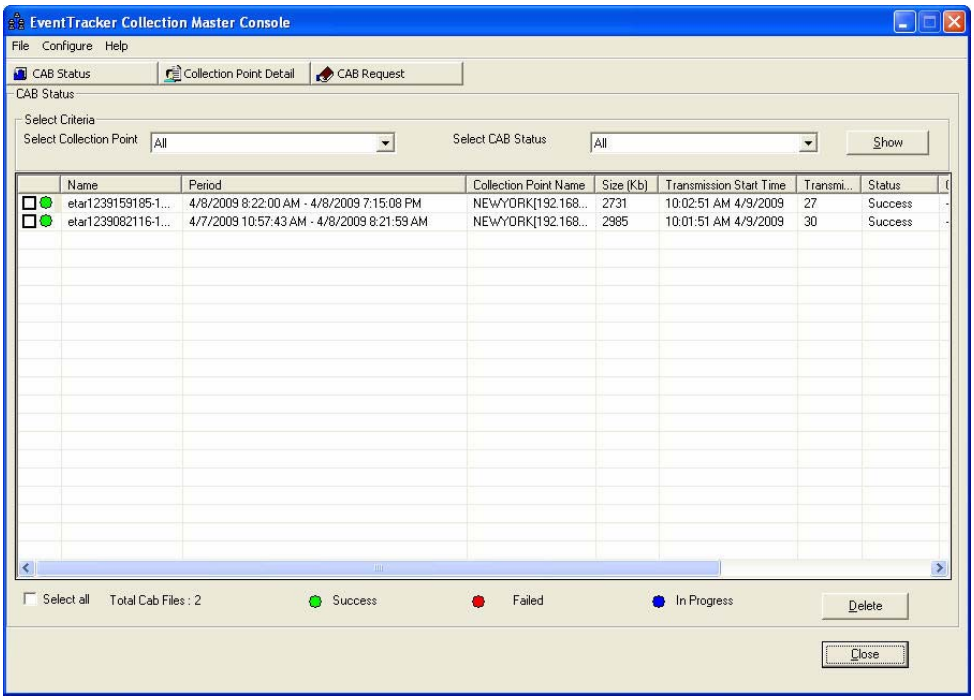


Table 74

Field	Description
Select Criteria	
Select Collection Point	Select Collection Point from this drop-down list. All Collection Points reporting to the Collection Master are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click **Show**. Available options are **All**, **Success**, **Failed** and **In Progress**.

Table 75

Field	Description
Name	Displays name of the CAB files.
Period	Displays the start time and end time. Start time is the date and time of the first event and end time is the date and time of the last event in the CAB file.
Collection Point Name	Displays name of the Collection Points. Select the Collection Point from Select Collection Point drop-down. EventTracker displays all the CAB files sent and being sent by the selected Collection Point. You can also set filter criteria by selecting appropriate option from Select CAB Status drop-down list.
Size (Kb)	Displays size of the CAB files.
Transmission Start Time	Displays date and time when the Collection Point started sending the CAB files.
Transmission Time (In Sec)	Displays time taken in seconds to send the CAB files.
Status	Displays status of the CAB files.
Comments	Reason for failure in receiving the CAB files is displayed in this column. For Success and In Progress, no comment is displayed.
Total Cab Files	Displays total number of CAB Files received from All Collection Points or Collection Point selected from the Select Client drop-down list.

Table 76

Icon	Represents
	CAB files received successfully by the Collection the Master.
	CAB files not received successfully by the Collection Master.
	CAB files being received by the Collection Master.

2 Select a Collection Point from the **Select Collection Point** drop-down list.

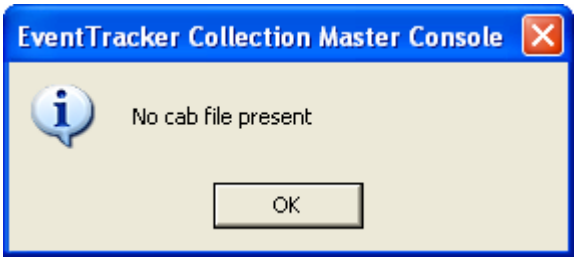
3 Select the status from the **Select CAB Status** drop-down list. Example; In Progress.

4 Click **Show**.

EventTracker displays the **CAB Status**.

EventTracker displays the status of the CAB files for the selected Collection Point in the CAB Status window. If there is no CAB file that meets the selected status criteria, then EventTracker displays the message box.

Figure 402 EventTracker Collection Master Console message box



Configuring Collection Master listening port

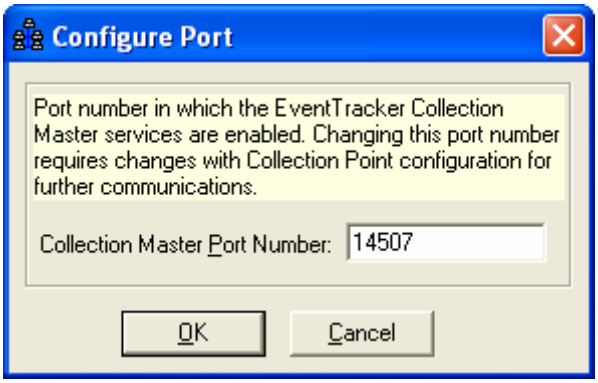
This option helps you configure listening port of the Collection Master. By default, EventTracker Collection Master and Collection Points communicate through port 14507. You can configure this port number from the Collection Master Console. If you configure a new port other than the default one, you have to configure at the Collection Points with the same port number for successful communication between the Collection Points and Collection Master.

To configure Collection Master listening port

1. Click the **Configure** menu and then select **Port Number**.

   EventTracker displays the Configure Port dialog box.

Figure 403 Configure Port dialog box


Configure Port
Port number in which the EventTracker Collection Master services are enabled. Changing this port number requires changes with Collection Point configuration for further communications.
Collection Master Port Number:
14507
OK
Cancel

2. Type the port number in the **Collection Master Port Number** field and then click **OK**.

Merging Collection Points – default Archives folder

To store the CAB files received from the Collection Points, Collection Master creates a new folder locally in the default EventTracker installation folder typically **…\Program Files\Prism Microsystems\EventTracker\Archives** with the respective name you type in **Site Name** field while installing Collection Points.

Scenario 1

Collection Master: WEBDOC1

IP Address: 192.168.1.88

Collection Point: NEWYORK. Consider this is the Site Name that you have entered while installing the Collection Point.

IP Address: 192.168.1.38

Collection Master creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\NEWYORK[192.168.1.38] and stores all the CAB files in that folder.

Now, uninstall the Collection Point and install it again on the same computer, however, this time with the Location Name NY. Send the Cab files to the Collection Master.

Collection Master creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\NY[192.168.1.38] and stores all the CAB files in that folder.

Although the CAB files are received from the same IP address, Collection Master creates different folders with the Site Name of the Collection Point and treats them as two different Sites.

To merge these two Sites, Open the Collection Master Console, click Collection Point Detail on the toolbar, select both the Collection Points (NEWYORK[192.168.1.38], NY[192.168.1.38]) and then click **Merge**.

Points to remember:

1. Old folder merges with the new folder.
2. While merging, Collection Master prompts you whether to overwrite the redundant CAB files or not.

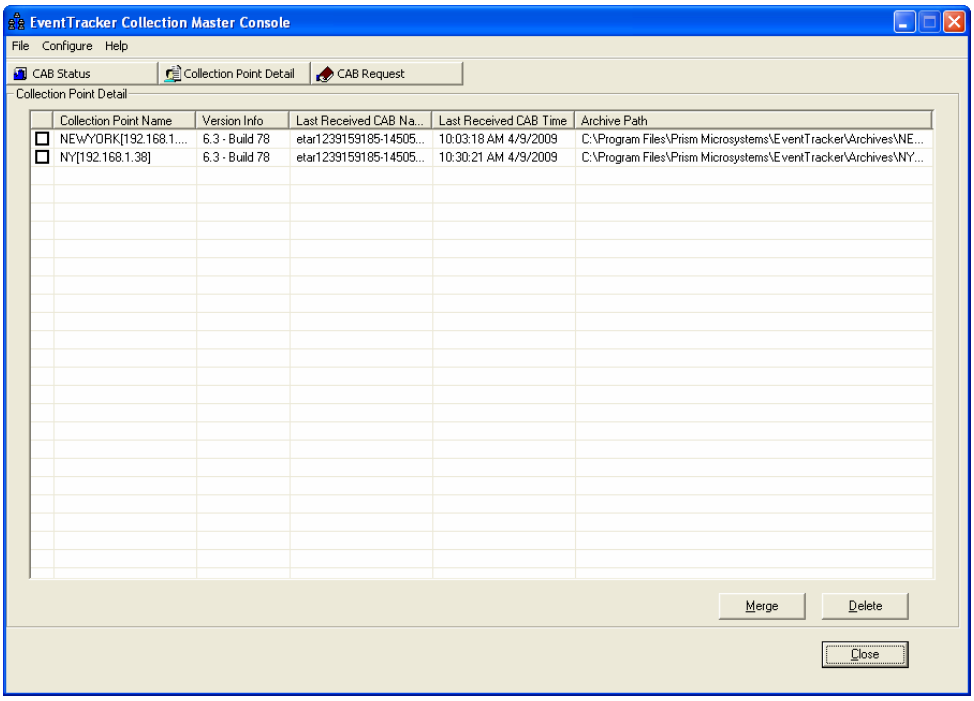
This option helps you merge two Collection Points.

To merge Collection Points

1. Click **Collection Point Detail** on the Collection Master Console.

   EventTracker displays the Collection Point Detail.

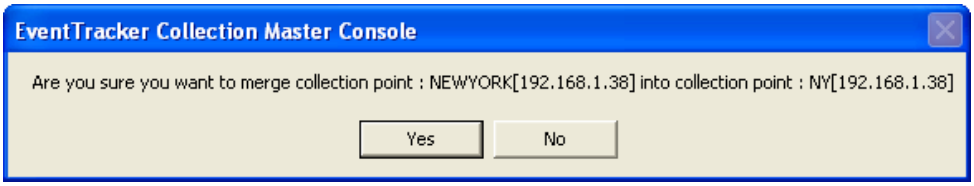
Figure 404 Collection Point Detail



2 Select the Collection Points and then click **Merge**.

EventTracker displays the confirmation message box.

Figure 405 Confirmation message box


EventTracker Collection Master Console
Are you sure you want to merge collection point : NEWYORK[192.168.1.38] into collection point : NY[192.168.1.38]
Yes
No

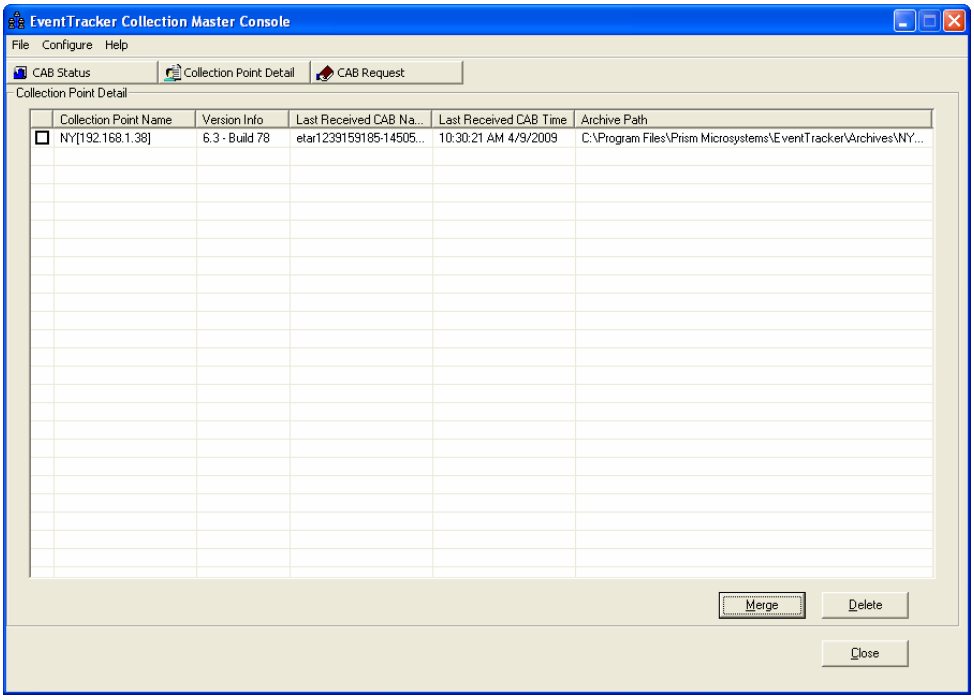
3 Click **Yes**.

EventTracker displays confirmation message box.

4 Click appropriately. Example **Yes to All**. Collection Master overwrites all the redundant CAB files.

EventTracker displays Collection Point Detail.

Figure 406 Collection Point Detail



Note

In this scenario, only the Collection Points are merged and the Collection Master copies the CAB files from … \Program Files\Prism Microsystems\EventTracker\Archives\ NEWYORK[192.168.1.38] to … \Program Files\Prism Microsystems\EventTracker\Archives\NY[192.168.1.38] folder. **CAB files of the Collection Master remain in the same archives folder … \Program Files\Prism Microsystems\EventTracker\Archives**. When you generate Reports for the Collection Point, EventTracker fetches CAB files from the NY[192.168.1.38] folder.

Scenario 2

Collection Master: WEBDOC1

IP Address: 192.168.1.88

Collection Point: NEWYORK. Consider this is the Site Name that you have given while installing Collection Point.

IP Address: 192.168.1.38

Collection Point: BOSTON. Consider this is the Site Name that you have given while installing Collection Point.

IP Address: 192.168.1.100

Collection Master creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\ NEWYORK[192.168.1.38] and stores all the CAB files received from NewYork in that folder.

Collection Master creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\BOSTON[192.168.1.100] and stores all the CAB files received from Boston in that folder.

To merge these two Sites, Open the Collection Master Console, click Collection Point Detail on the toolbar, select the Collection Points, and then click **Merge**.

Points to remember:

1. Old folder merges with the new folder.
2. While merging, Collection Master prompts you whether to overwrite the redundant CAB files or not.

Scenario 3

Collection Master: WEBDOC1

IP Address: 192.168.1.88

Collection Point: NEWYORK. Consider this is the Site Name that you have given while installing Collection Point.

IP Address: 192.168.1.38

Collection Point creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\ NEWYORK[192.168.1.38] and stores all the CAB files in that folder.

Now, uninstall the Collection Point and install it again on the same computer with the same Site Name NEWYORK. Send the Cab files to the Collection Master.

Collection Point retains the old folder … \Program Files\Prism Microsystems\EventTracker\Archives\ NEWYORK[192.168.1.38] and stores all the CAB files in that folder.

Point to remember:

- Collection Master backs up the older files with the same name but appends timeticks. Timeticks is the time when the Collection Master received the new CAB files.

Merging Collection Points – modified Archives folder

COLLECTION MASTER CAB FILES

When you modify the default archives path, Collection Master stores the new CAB files in the new Archives folder. You have to manually copy all the old CAB files to the new Archives folder. When you generate Advanced Reports, EventTracker refers to the CAB files located in the new Archives folder.

Before you attempt to manually copy the CAB files from old Archives folder to the new Archives folder, do the following:

1. Stop the EventTracker services in the same order as given below.
   - EventTracker Agent
   - EventTracker EventVault
   - EventTracker Scheduler
2. Apply the patch ET63P09-056.exe
3. Create a new folder typically "Archives." Example: D:\Archives
4. Copy the VCP folder structure and paste to the new Archives folder.

   Suppose the VCP folder structure is as follows,

   C:\Program Files\Prism Microsystems\EventTracker\Archives\14505

   C:\Program Files\Prism Microsystems\EventTracker\Archives\14509

   C:\Program Files\Prism Microsystems\EventTracker\Archives\514

   Copy the folders 14505, 14509, and 514 and paste them to the new Archives folder.

   It should be similar as follows

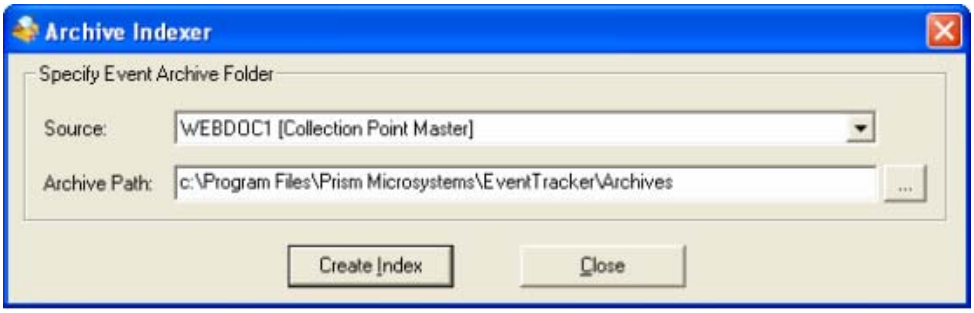
   D:\Archives\14505

   D:\Archives\14509

   D:\Archives\514
5. Double-click Maintenance Tools on the Control Panel.
6. Double-click Archive Indexer.

   EventTracker displays the Archive Indexer.

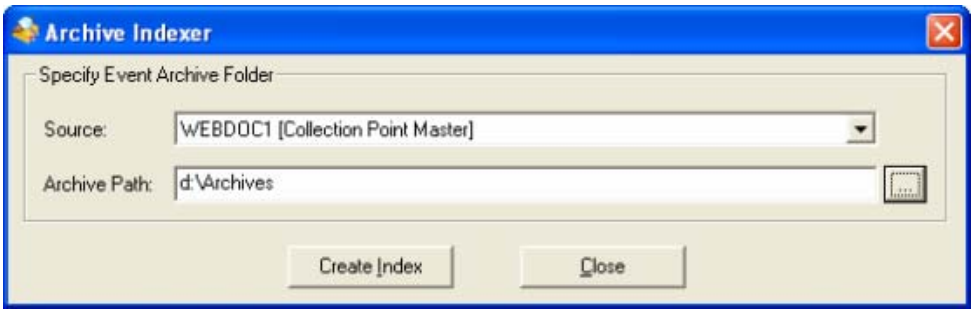
Figure 407 Archive Indexer



7 Select the Source as your Collection Master system.

8 Click the browse button and select the new Archives folder.

Figure 408 Archive Indexer



9 Click Create Index.

Archive Indexer creates the index file (etwarindex.mdb) in the new Archives folder.

10 Open the EventVault Warehouse Manager console and select the "Archives" folder in the Configuration window. Example: D:\Archives

11 Restart the EventTracker services.

Caution: Do not disturb the Collection Point CAB files. To move Collection Point CAB files, you have to merge the Collection Points.

Note

If any Scheduled Reports run in the background during this migration period, they might fail. However, the EventTracker Scheduler will pick them up for processing in the next schedule time and it will refer to the new Archives folder for CAB files.

COLLECTION POINT CAB FILES

Collection Master creates a new folder in the default EventTracker installation folder typically …\Program Files\Prism Microsystems\EventTracker\Archives with the respective name you enter in Site or group name field, while installing Collection Points, to store the CAB files received from the Collection Points.

Example: …\Program Files\Prism Microsystems\EventTracker\Archives\ALICE-II[192.168.1.53]

Collection Master creates a new folder in the modified archives folder and stores the new CAB files received from the Collection Point in that folder. If you want to merge Collection Points, use the "Merge" option in the Collection Master Console. When you generate Advanced Reports, EventTracker fetches the CAB files from the new Archives folder.

Note

Collection Master will not delete the old Archives folder. It is left to your discretion to handle the old folder.

Scenario 1

Collection Master: WEBDOC1

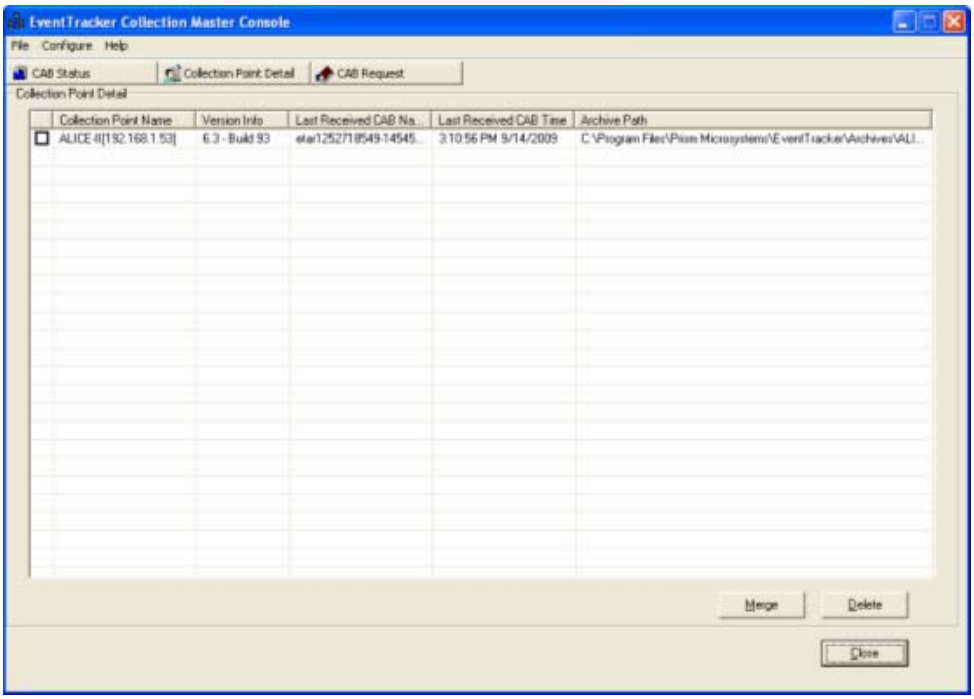
IP Address: 192.168.1.88

Collection Point: ALICE-II. Consider "ALICE-II" is the Site or group name that you have entered while installing the Collection Point.

IP Address: 192.168.1.53

Collection Master creates a folder …\Program Files\Prism Microsystems\EventTracker\Archives\ ALICE-II[192.168.1.53] and stores all the CAB files in that folder.

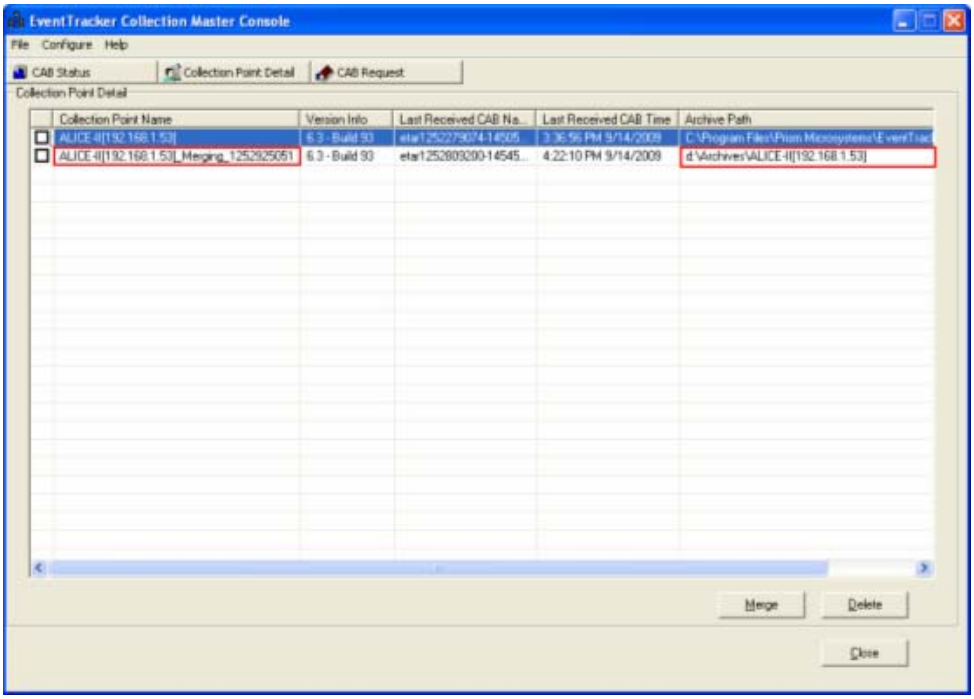
Figure 409 Collection Point Detail



Now, modify the Archives folder in the Collection Master as explained in the previous section. Send the Cab files to the Collection Master.

Collection Master creates a folder D:\Archives\ALICE-II[192.168.1.53] and stores all new CAB files in that folder.

Figure 410 Collection Point Detail



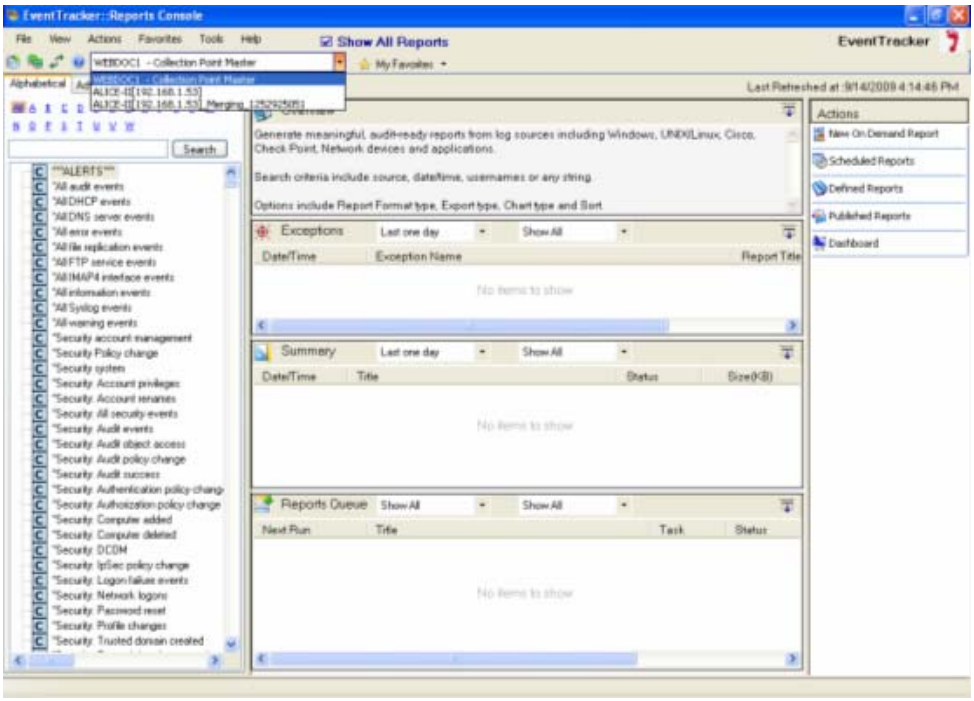
Since the Collection Point name remains the same before and after changing the Archives path, Collection Master appends Merging and Timeticks to the Collection Point name. EventTracker provides this naming convention to avoid Collection Point name conflicts.

Example: ALICE-II[192.168.1.53] (default Archives path)

ALICE-II[192.168.1.53]_Merging_1252925051 (modified Archive path)

ALICE-II[192.168.1.53]_Merging_1252925051 is visible when you generate Advanced Reports.

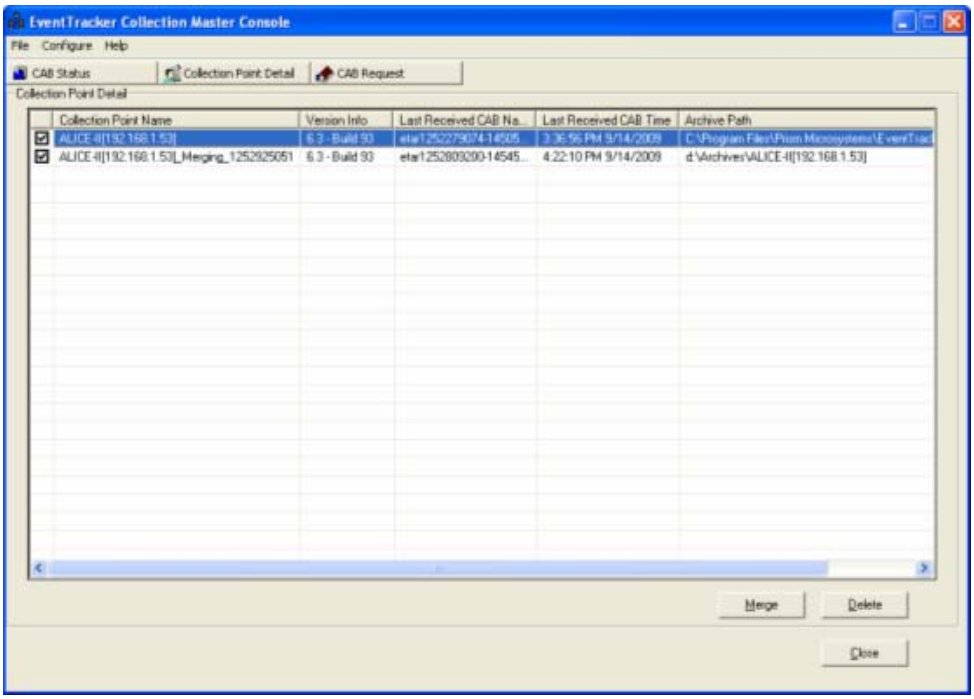
Figure 411 Advanced Reports console



Had you configured Scheduled Reports, the Advanced Report console might still be referring to the CAB files in the old folder. So you are required to merge these two sites before you attempt to generate Advanced Reports.

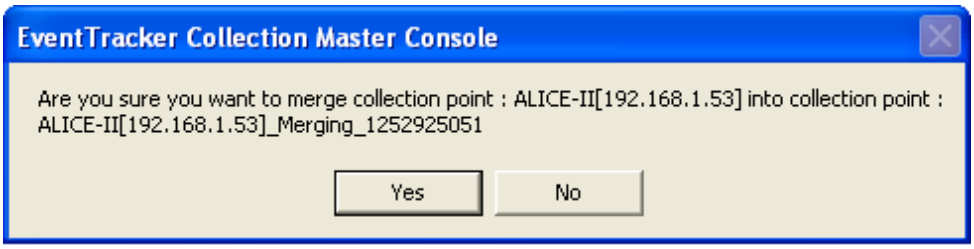
To merge these two Sites, Open the Collection Master Console, click Collection Point Detail on the toolbar, select both the Collection Points and then click **Merge**.

Figure 412 Collection Point Detail



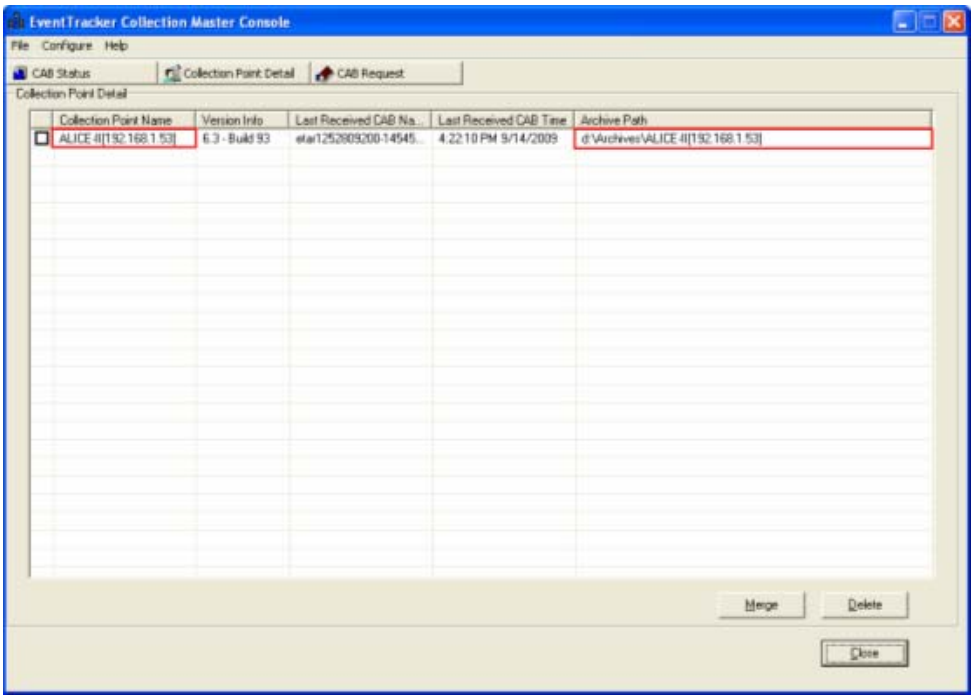
Collection Master Console displays the confirmation message box.

Figure 413 Collection Master Console message box


EventTracker Collection Master Console
Are you sure you want to merge collection point : ALICE-II[192.168.1.53] into collection point : ALICE-II[192.168.1.53]_Merging_1252925051
Yes
No

Click **Yes** to merge the Collection Points.

Figure 414 Collection Points after merging



When you merge the Collection Points,

- Collection Master will retain the CAB files intact in the default Archives folder …\Program Files\Prism Microsystems\EventTracker\Archives\ALICE-II[192.168.1.53]
- Moves the CAB files from the default Archives folder to the new Archives folder d:\Archives\ALICE-II[192.168.1.53].
- Updates the Index file
- Extracts the CAB files from the new Archives folder so that the report schedules remain intact.

Points to remember:

1. Old folder merges with the new folder.
2. While merging, Collection Master prompts you whether to overwrite the redundant CAB files or not.

Scenario 2

Collection Master: WEBDOC1

IP Address: 192.168.1.88

Collection Point: ALICE-II. Consider this is the Site or group name that you have entered while installing the Collection Point.

IP Address: 192.168.1.53

Collection Master creates a folder … \Program Files\Prism Microsystems\EventTracker\Archives\ ALICE-II[192.168.1.53] and stores all the CAB files in that folder.

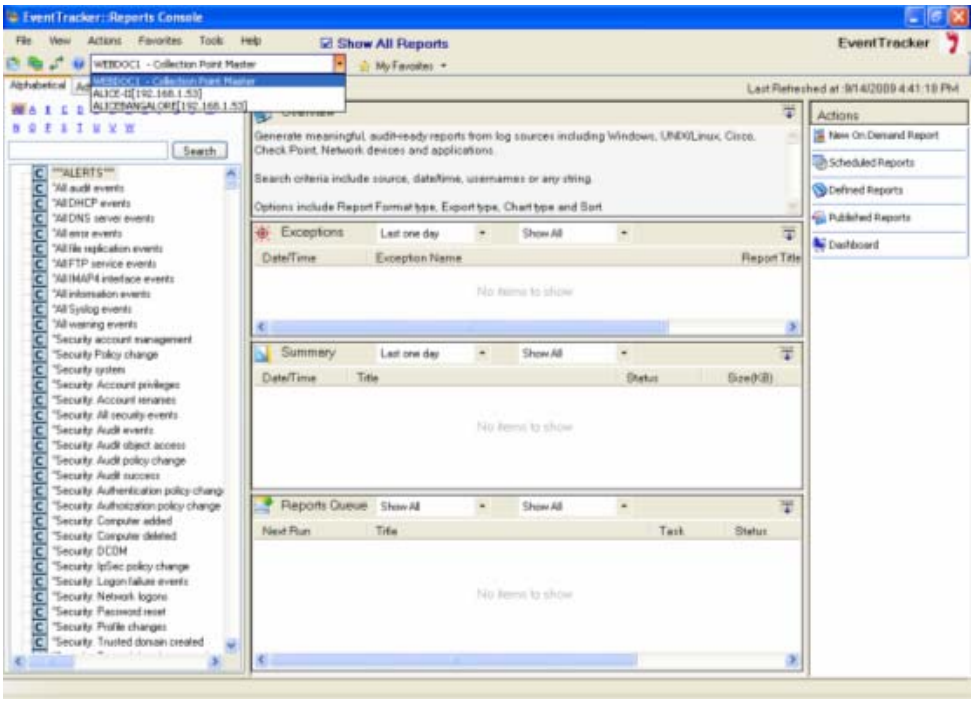
Now, modify the Archives folder in the Collection Master end. Example: D:\Archives.

Change the Collection Point Site or group name as ALICEBANGALORE and send the CAB files to the Collection Master.

Collection Master creates a folder D:\Archives\ ALICEBANGALORE[192.168.1.53] and stores all the new CAB files in that folder.

Generate an Advanced Report. Advanced Reports Console displays both the Collection Points.

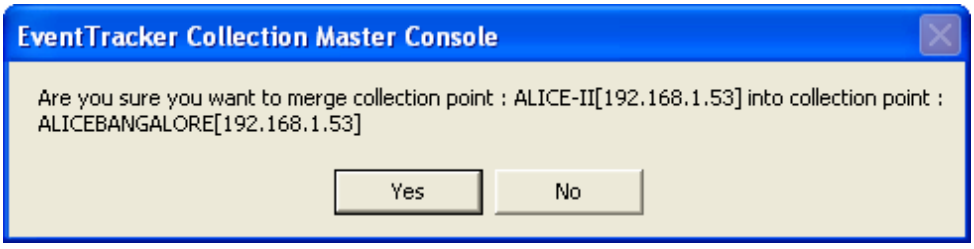
Figure 415 Advanced Reports Console



To merge these two Sites, Open Collection Master Console, click Collection Point Detail on the toolbar, select both the Collection Points and click Merge.

Collection Master displays the confirmation message box.

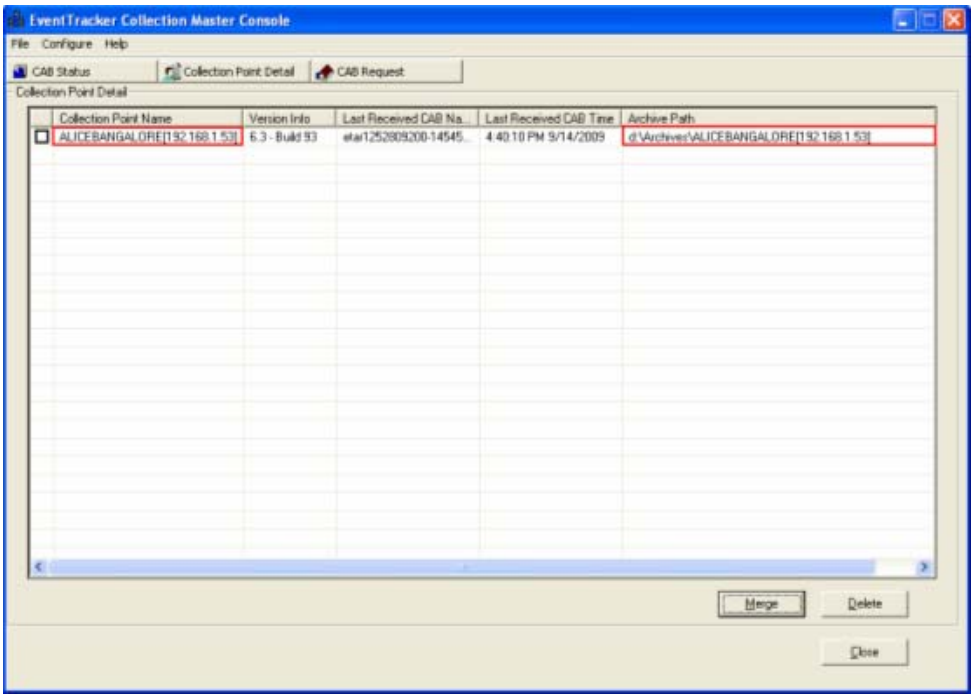
Figure 416 Collection Master Console message box


EventTracker Collection Master Console
Are you sure you want to merge collection point : ALICE-II[192.168.1.53] into collection point : ALICEBANGALORE[192.168.1.53]
Yes
No

Click **Yes** to merge the Collection Points.

Collection Master displays the Collection Point Detail after merging the Collection Points.

Figure 417 Collection Points after merging



When you merge the Collection Points,

- Collection Master will retain the CAB files intact in the default Archives folder
- Moves the CAB files from the default Archives folder to the new Archives folder.
- Updates the Index file
- Extracts the CAB files from the new Archives folder so that the report schedules remain intact.

Points to remember:

1. Old folder merges with the new folder.
2. While merging, Collection Master prompts you whether to overwrite the redundant CAB files or not.

Requesting CAB files

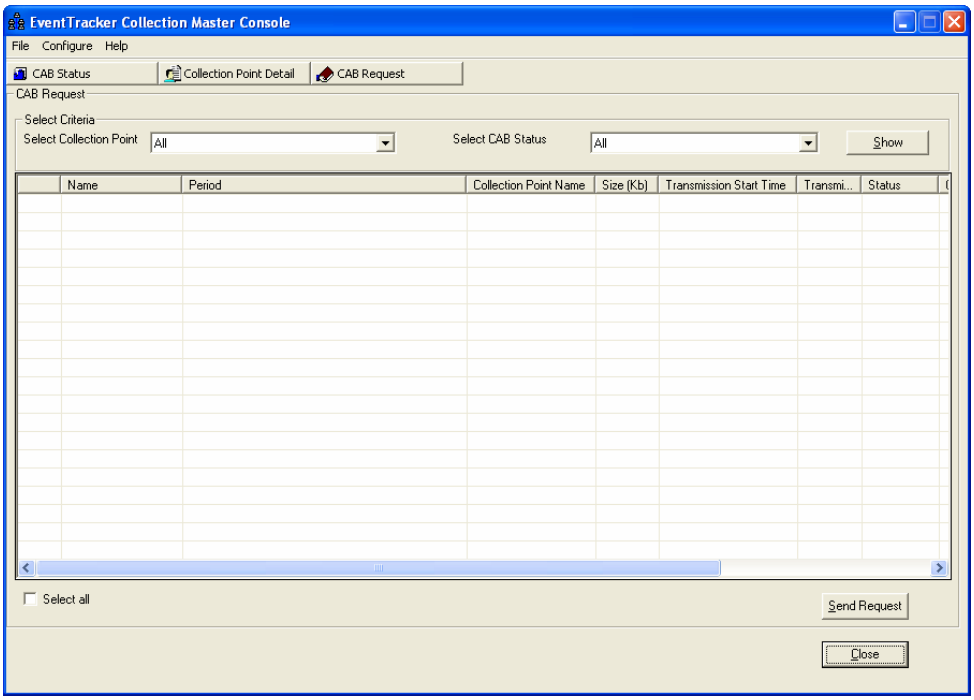
This option helps you send a request to the Collection Point(s) for the CAB files missing in the archives or the CAB files that were failed to transfer. The files are missing may be you would have inadvertently deleted them.

To request CAB files

1. Open the Collection Master Console.
2. Click **CAB Request**.

   EventTracker displays the CAB Request window.

Figure 418 CAB Request



Note

The CAB Request screen is empty, since there is no missing or failed to transfer CAB files.

Table 77

Field	Description
Select Criteria	
Select Collection Point	Select Collection Point from this drop-down list. All Collection Points reporting to the Collection Master are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click **Show**. Available options are **All**, **Missing in Source**, and **Failed to Transfer**.

Table 78

Field	Description

Field	Description
Name	Displays name of the CAB files.
Period	Displays the start time and end time. Start time is the date and time of the first event and end time is the date and time of the last event in the CAB file.
Collection Point Name	Displays name of the Collection Points. Select the Collection Point from Select Collection Point drop-down. EventTracker displays all the CAB files sent and being sent by the selected Collection Point. You can also set filter criteria by selecting appropriate option from Select CAB Status drop-down list.
Size (Kb)	-
Transmission Start Time	-
Transmission Time (In Sec)	-
Status	Displays status of the CAB files as **Missing** or **Failed**.
Comments	Reason for failure in receiving the CAB files is displayed in this column. For Success and In Progress, no comment is displayed.
Total Cab Files	Displays total number of CAB Files selected for request.

Table 79

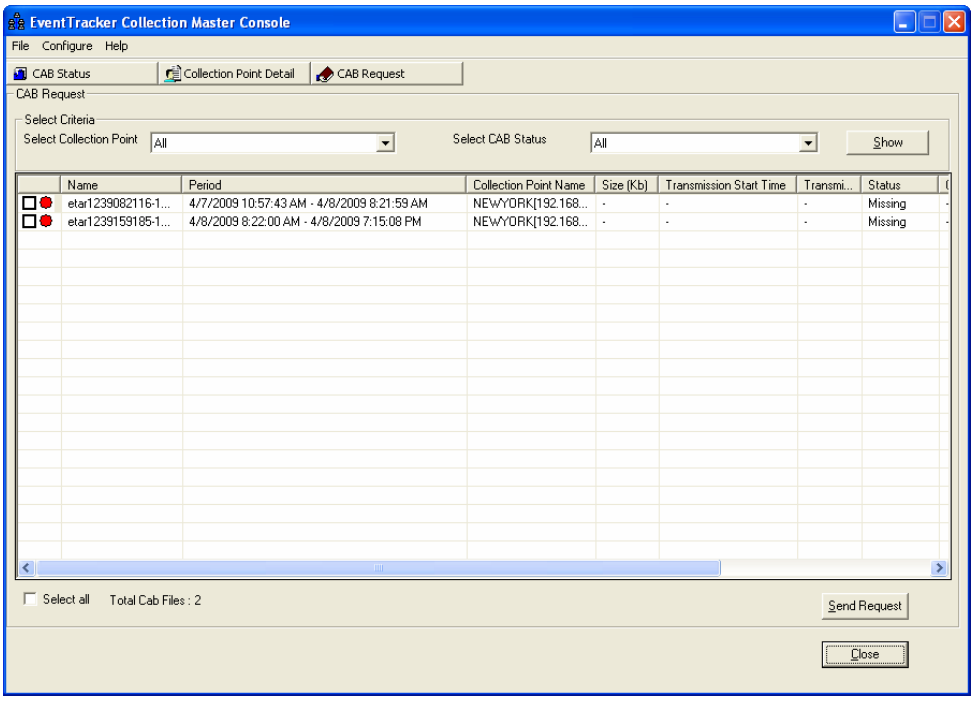
Icon	Represents
	CAB files missing or failed to transfer.

To understand the functionality of CAB Request, delete some CABs from the Archives folder and see what happens.

3 Open the Collection Master Console and click CAB Request.

EventTracker displays the CAB Request window with the details of missing CAB files.

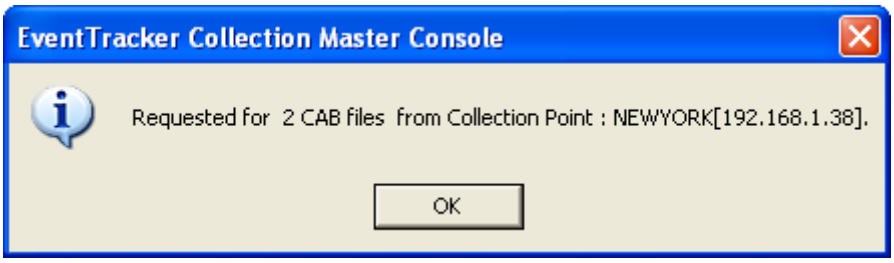
Figure 419 CAB Request



4 You can select individual files or click **Select All** to select all the files and then click **Send Request**.

EventTracker displays the Collection Master Console message box.

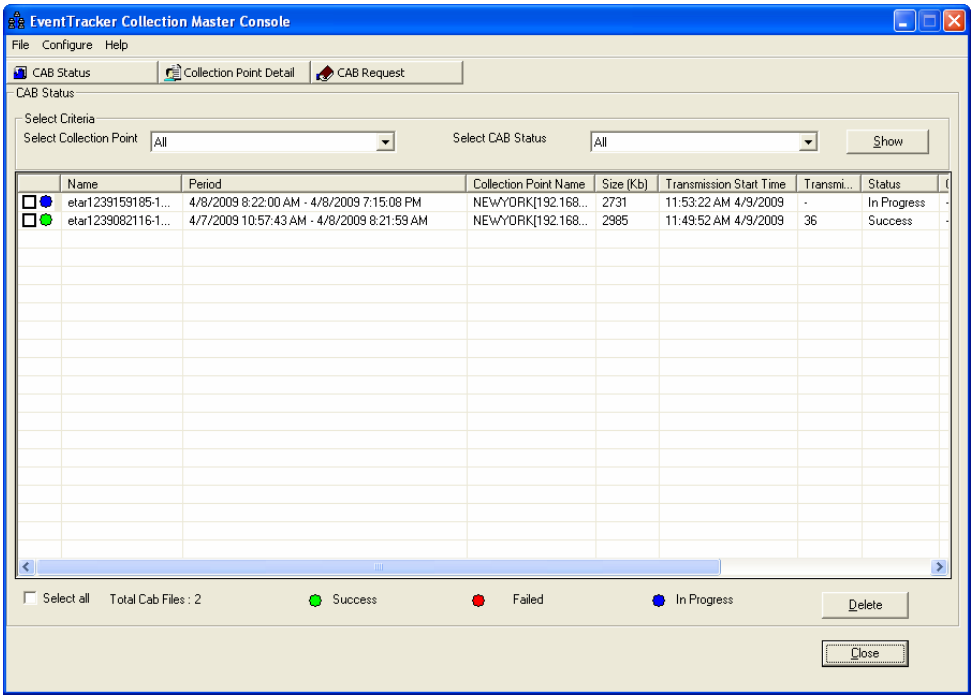
Figure 420 Collection Master Console message box



5 Click **OK**.

Collection Master send the request, receives the missing CAB files from the concerned Collection Point and displays the CAB Status screen.

Figure 421 CAB Request



Deleting CAB files

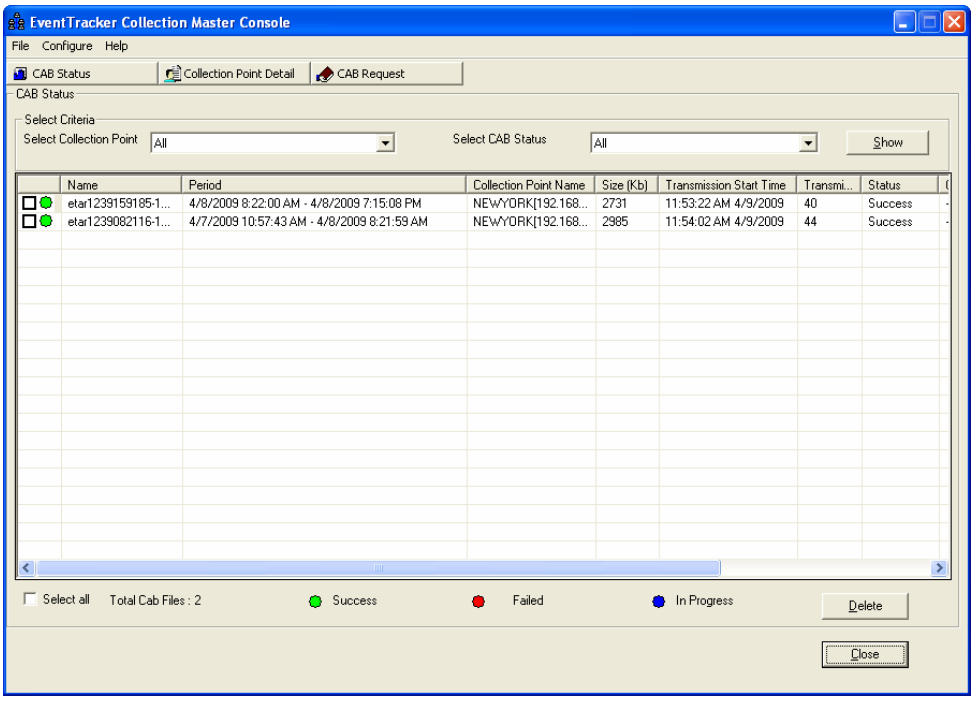
This option helps you delete CAB files.

To delete CAB files

1 Click **CAB Status** on the Collection Master Console.

EventTracker displays CAB Status.

Figure 422 CAB Status



2 Select the **Select All** check box to select all CAB files for deletion.

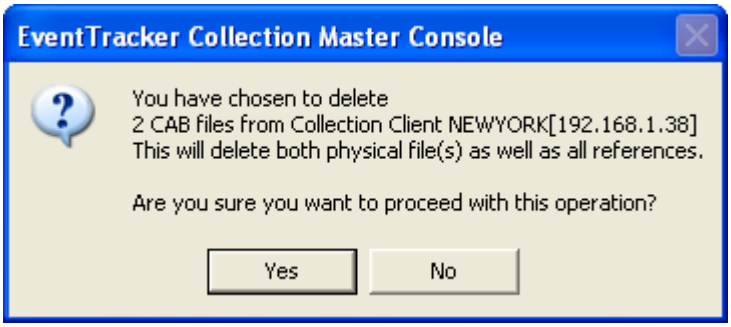
(OR)

Select the check box against individual CAB files that you want to delete.

3 Click **Delete**.

EventTracker displays the confirmation message box.

Figure 423 Confirmation message box


EventTracker Collection Master Console
You have chosen to delete
2 CAB files from Collection Client NEWYORK[192.168.1.38]
This will delete both physical file(s) as well as all references.
Are you sure you want to proceed with this operation?
Yes
No

4 Click **Yes**.

EventTracker deletes the selected CAB file.

Deleting Collection Point Detail

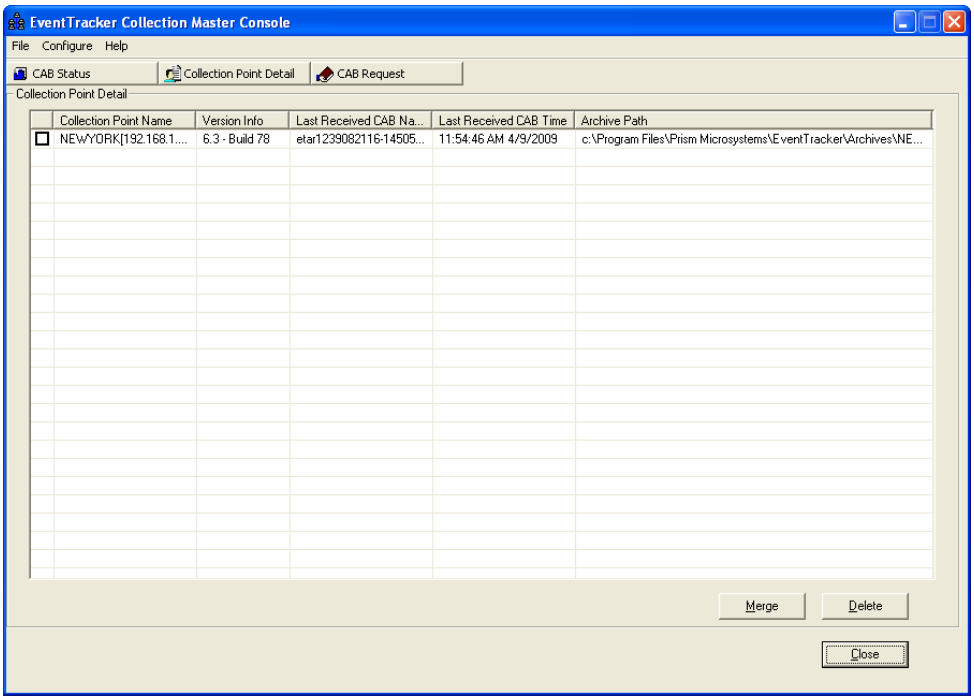
This option helps you delete Collection Point details.

To delete Collection Point detail

1 Click **Collection Point Detail** on the Collection Master Console.

EventTracker displays the Collection Point Detail.

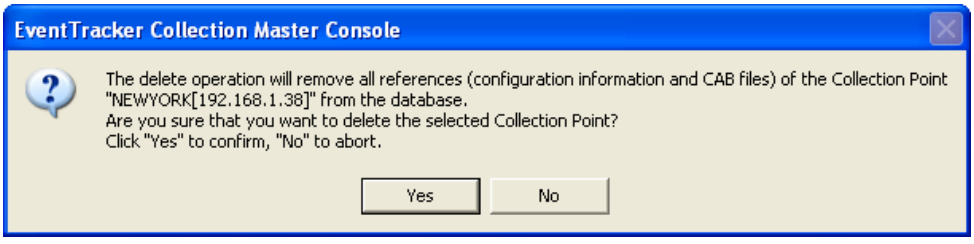
Figure 424 Collection Point Detail



2 Select the Collection Point detail that you want to delete and then click **Delete**.

EventTracker displays the confirmation message box.

Figure 425 Confirmation message box

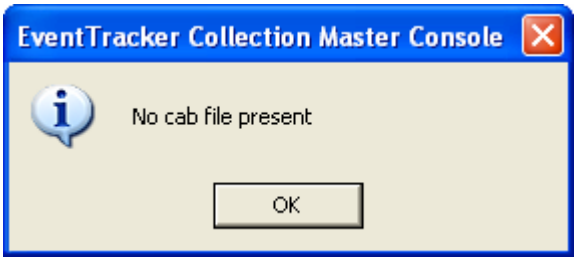

EventTracker Collection Master Console
The delete operation will remove all references (configuration information and CAB files) of the Collection Point "NEWYORK[192.168.1.38]" from the database.
Are you sure that you want to delete the selected Collection Point?
Click "Yes" to confirm, "No" to abort.
Yes
No

3 Click **Yes**.

4 Click **CAB Status** on the Collection Master Console.

EventTracker displays the message box.

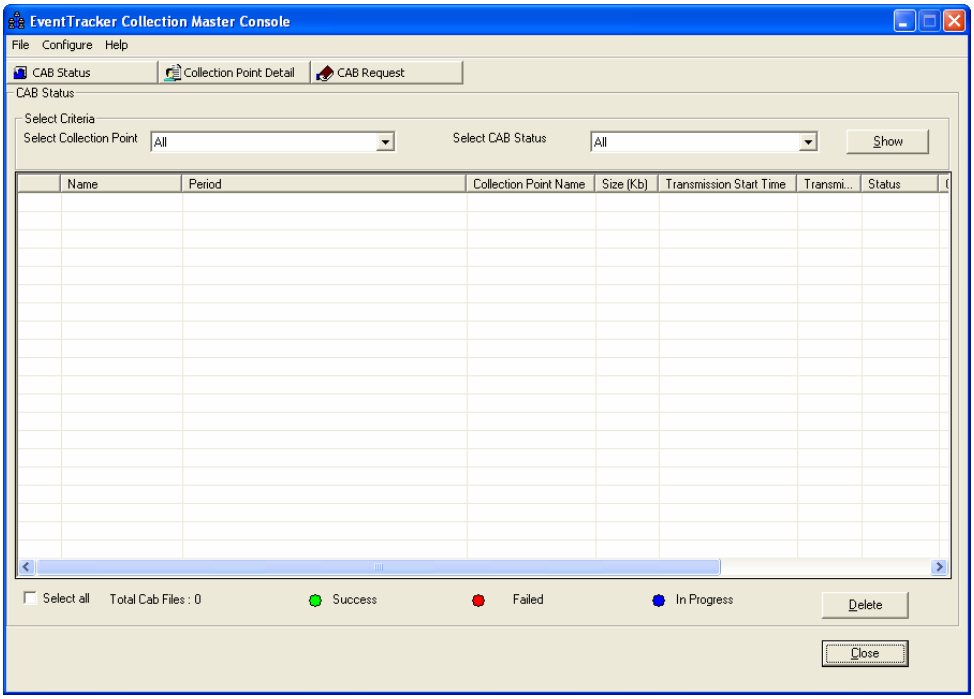
Figure 426 Collection Master Console message box



5 Click **OK**.

EventTracker displays the Collection Master Console.

Figure 427 Collection Master Console



Note

When you delete Collection Point details, EventTracker deletes all the CAB files received from the deleted Collection Points.

Configuring Alerts

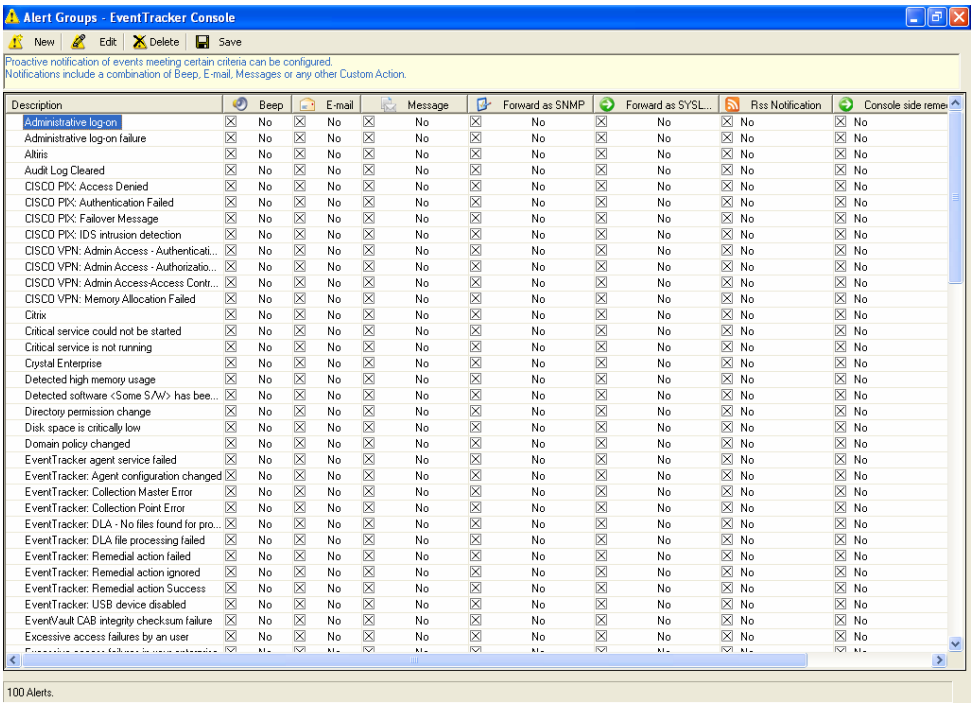
Two new Alerts namely, **EventTracker: Collection Master Error** and **EventTracker: Collection Point Error** have been added exclusively for Collection Point model. You can configure those Alerts in the **Alert Groups** console to send you notifications. It is not possible to get alert notification for Collection Master related errors in Collection Point and vice versa.

To configure Alerts

1. Open EventTracker Management Console.
2. Click the **Configure** menu and select the **Configure Alerts** option.

   EventTracker displays the Alert Groups console.

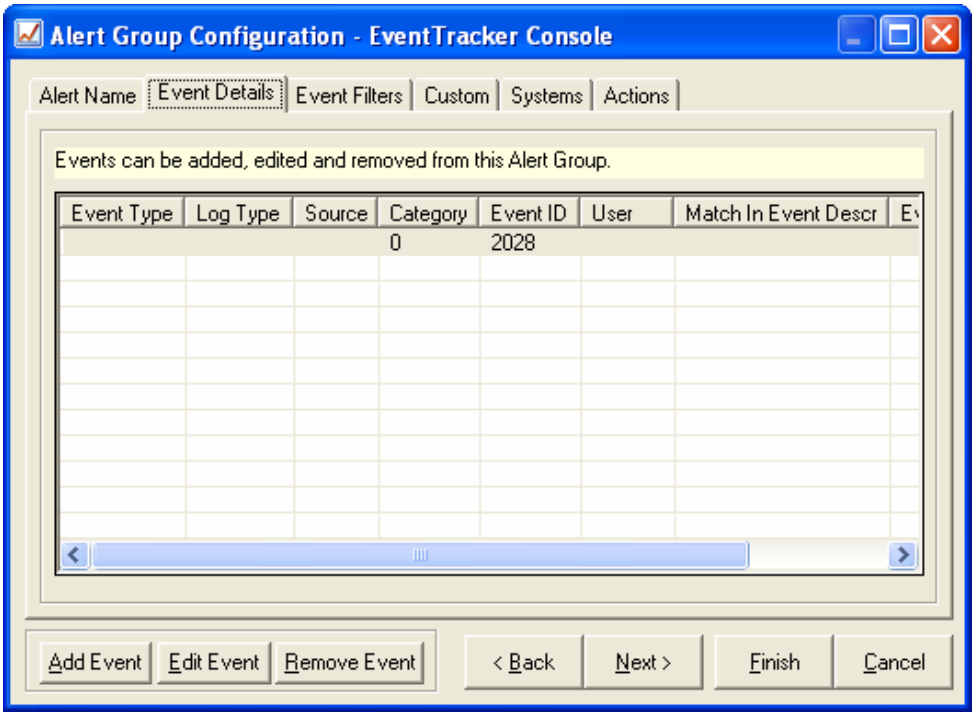
Figure 428 Alert Groups console



3. Double-click EventTracker: Collection Master Error.

   EventTracker displays Alert Group Configuration console.

Figure 429 Alert Group Configuration console



4 Select appropriate options in Event Filters, Custom, Systems, Actions tabs and then click F**inish**.

5 Click **Save** on the Alert Groups console.

EventTracker displays the EventTracker Management Console Message.

6 Click **OK**.

7 Restart the Management Console.

Chapter 16
Collection Point

In this chapter, you will learn how to:

- Starting Collection Point Console
- Add Collection Master
- Edit Collection Master Settings
- Delete Collection Master Settings
- View CAB Status
- Send CAB files to Collection Masters
- Set Purge Frequency

Starting Collection Point Console

This option helps you open Collection Point Console.

To open Collection Point Console

1. Open the Control Panel.

2. Double-click

(OR)

Click Start, point to Programs, point to Prism Microsystems, point to EventTracker, and then select **EventTracker Collection Point Configuration** option.

EventTracker displays the Collection Point Console.

Figure 430 Collection Point Console

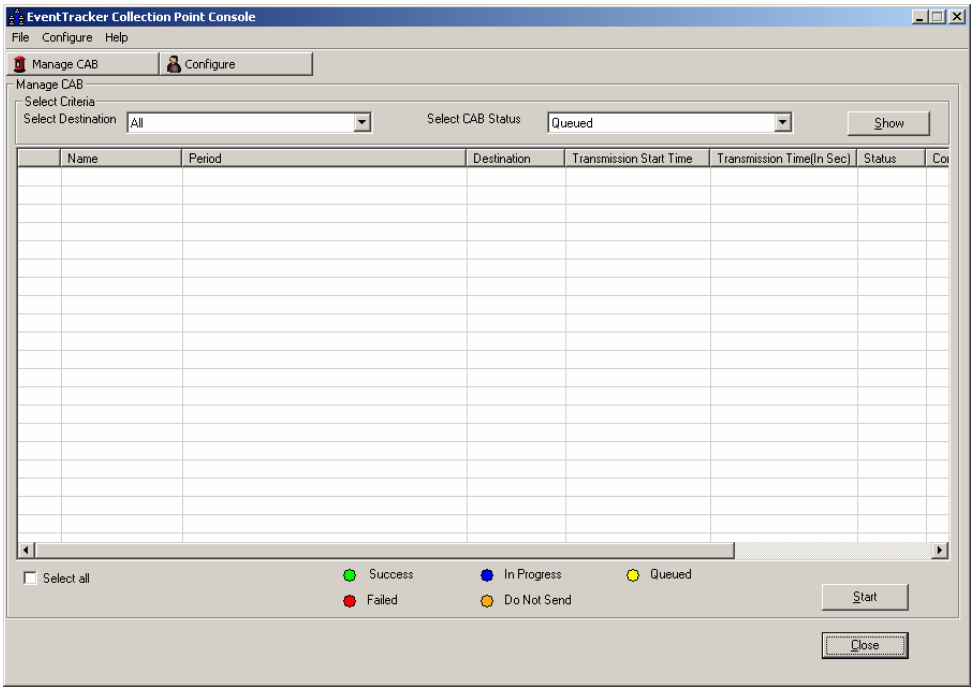


Table 80

Click	To
Configure Managers	Add Collection Masters.
Manage CAB	View status of all CAB files.

Table 81

Field	Description
Select Criteria	
Select Destination	Select the Collection Master from this drop-down list. Collection Masters that you have added are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click **Show**. Available options are **All**, **Success**, **Failed**, **Do not Send**, **In Progress** and **Queued**.
Select all	Select this check box to mark all the CAB files to send to the selected Collection Master(s).

Adding Collection Masters

This option helps you add Collection Masters.

Every Collection Point can be configured to send CAB files simultaneously up to 5 Collection Masters. The Collection Master may exist in the same domain or in the trusted domain.

To configure Collection Masters

1. Click **Configure** on the Collection Point Console.

   (OR)

   Click the **Configure** menu and then select **Manager**.

   EventTracker displays the Configure Managers console.

Figure 431 Configure Managers console

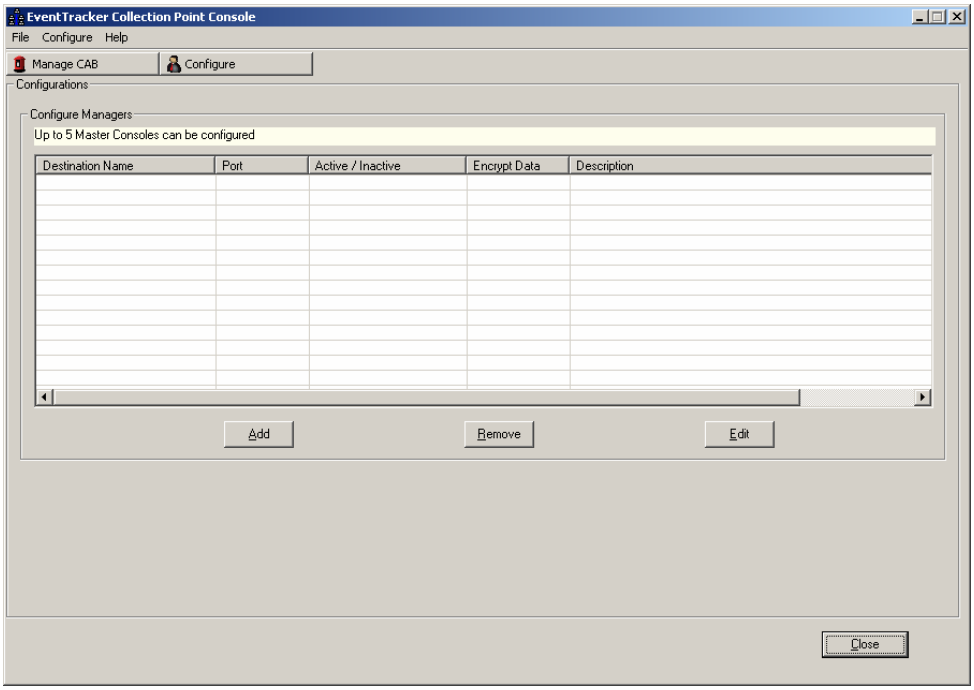


Table 82

Field	Description
Configure: Configured Collection Master(s) details are displayed in this console.	
Destination Name	Displays IP address of the configured Collection Master(s).
Port	Default port is 14507. You can modify the port number. Port numbers should be same on both the Collection Master and Collection Point.
Active / Inactive	Displays status of the Collection Master. Collection Point will not send CAB files to the Collection Master(s) that is Inactive.
Description	Displays description about the Collection Master(s).

Table 83

Click	To
Add	Add new managers.
Edit	Edit manager configuration settings.
Remove	Delete manager configuration settings.
Close	Close the window.

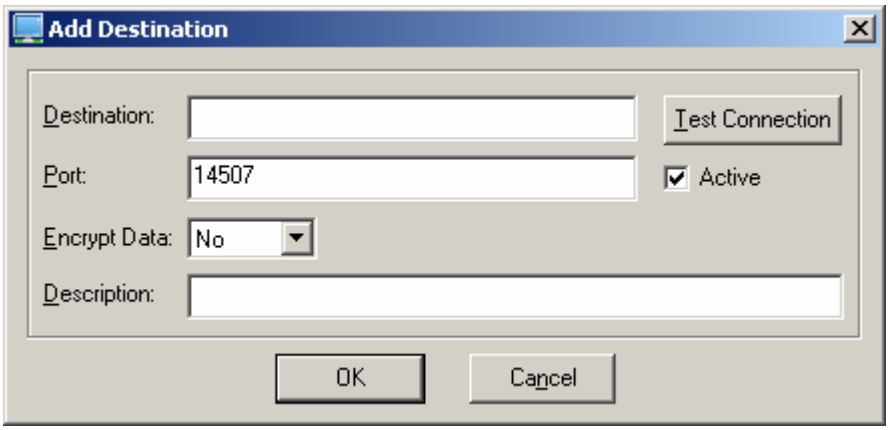
Note

Purge Archives older than: Archives will be purged after selected number of days. EventTracker Scheduler process will not purge the archives if the number of days is set to zero.

2 Click **Add**.

EventTracker displays the Add Destination dialog box.

Figure 432 Add Destination dialog box

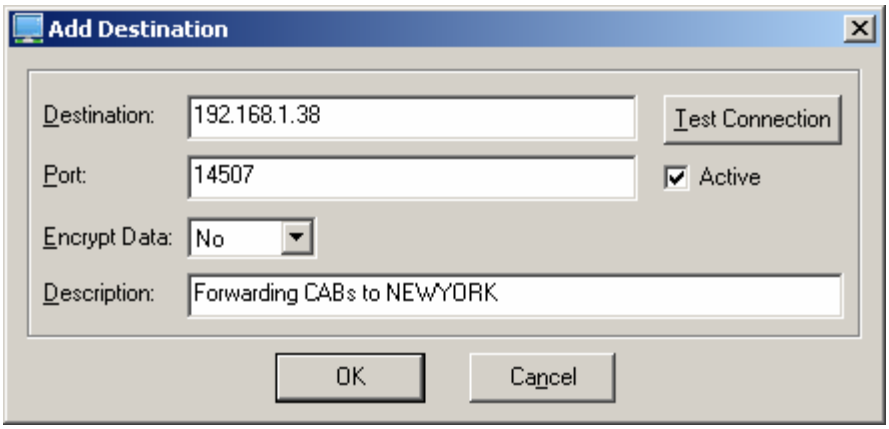


Note

EventTracker selects **Active** check box by default. When you clear this check box, Collection Point will not send CAB files to the Collection Master that you have deactivated. Collection Point can be configured to report up to 5 Collection Masters simultaneously. You can configure as many Collection Masters as possible and activate / deactivate them as the situations demand.

3 Enter/select appropriately in the relevant fields and then click **OK**.

Figure 433 Add Destination dialog box



Note

EventTracker accepts only numeric data type in **Port** field.

4 Click **Test Connection** to check connectivity between the Collection Point and the Collection Master.

EventTracker displays the message box.

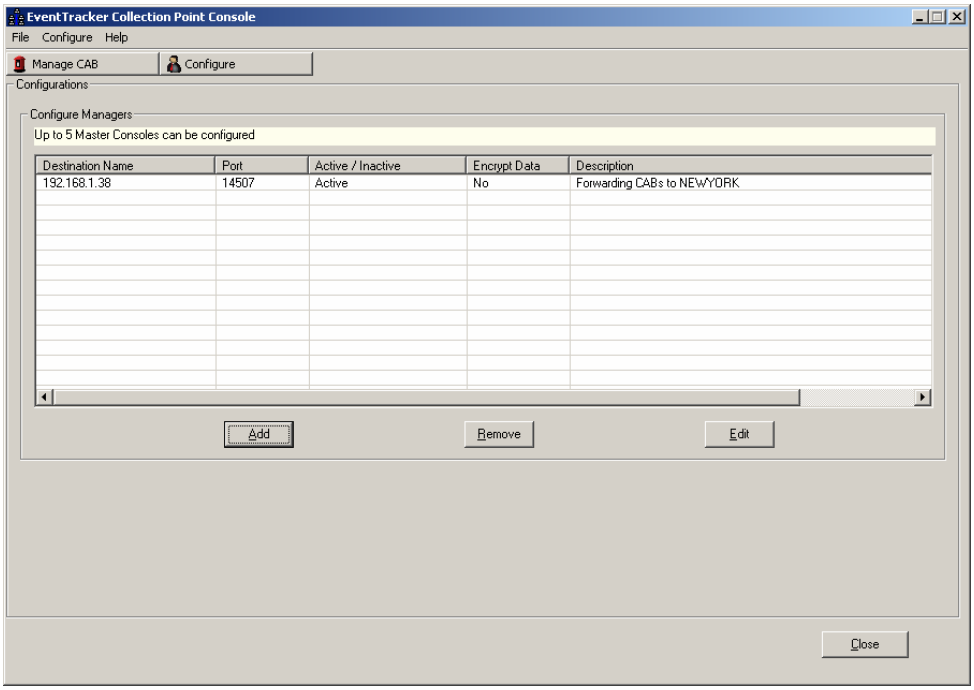
Figure 434 EventTracker Collection Point Console message box

5 Click **OK**.

6 Click **OK** on the Add Destination dialog box.

EventTracker displays the Configure Managers console with the newly configured Manager.

Figure 435 Configure Managers console



7 Click **Close** to close the window.

Editing Collection Master Settings

This option helps you edit Collection Master configuration settings.

To edit Collection Master configuration settings

1 Click **Configure** on the Collection Point Console.

(OR)

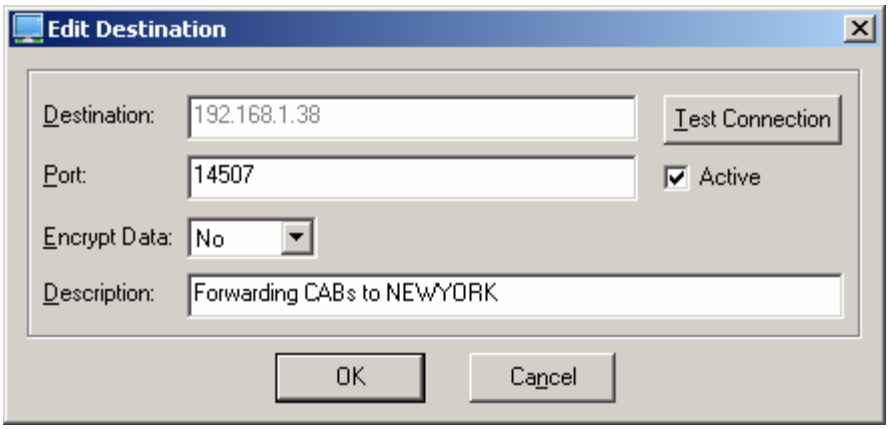
Click the **Configure** menu and then select **Manager**.

EventTracker displays the Configure Managers console.

2 Select the Collection Master and then click **Edit**.

EventTracker displays Edit Destination dialog box.

Figure 436 Edit Destination dialog box



You can edit, **Port**, **Description** and select or clear **Active** check box. Type changes appropriately in the relevant fields and then click **OK**.

Deleting Collection Master Settings

This option helps you delete Collection Master settings.

To delete Collection Master settings

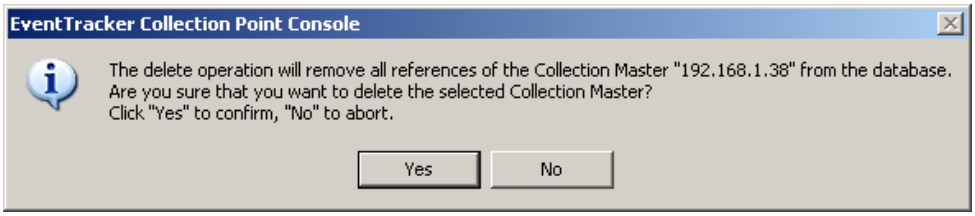
1. Click **Configure** on the Collection Point Console.

   EventTracker displays the Configure Managers console.

2. Select the Collection Master and then click **Remove**.

   EventTracker displays the confirmation message box.

Figure 437 Collection Point Console confirmation message box


EventTracker Collection Point Console
The delete operation will remove all references of the Collection Master "192.168.1.38" from the database.
Are you sure that you want to delete the selected Collection Master?
Click "Yes" to confirm, "No" to abort.
Yes
No

3. Click **Yes**.

   EventTracker deletes the selected Collection Master configuration settings.

Viewing CAB Status

This option helps you view status of the CAB files that are transferred and being transferred by the Collection Point to the Collection Master(s).

To view CAB status

1 Click **Manage CAB** on the Collection Point Console.

EventTracker displays the Manage CAB Console.

Figure 438 Manage CAB console

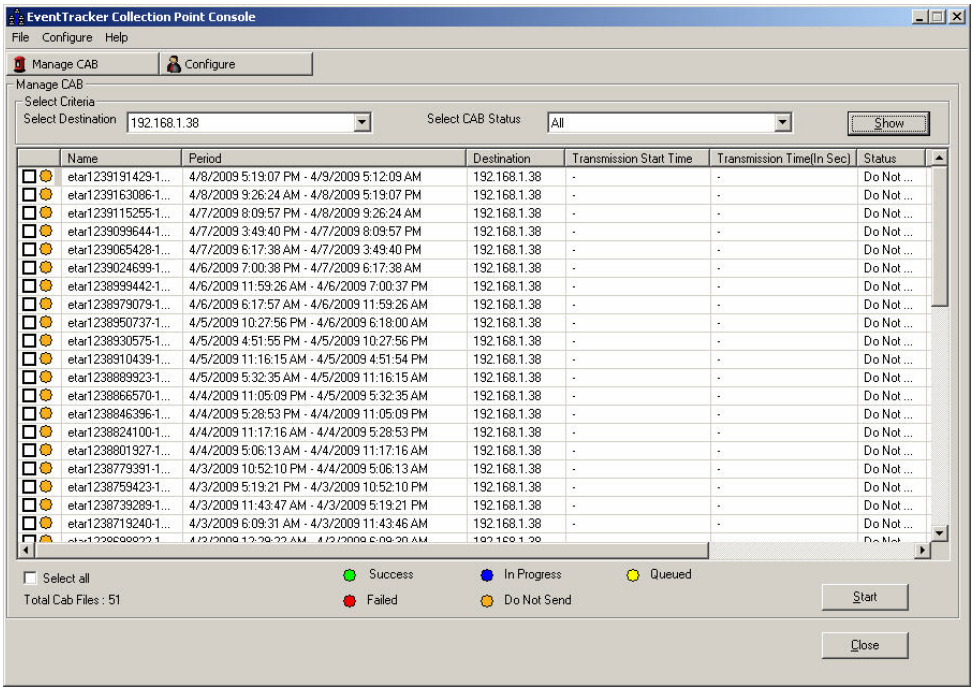


Table 84

Field	Description
Select Criteria	
Select Destination	Select Destination from the drop-down list. All configured Collection Masters are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click **Show**. Available options are **All**, **Success**, **Failed, Do Not Send, In Progress** and **Queued**.
Select All	Select this check box to mark all the CAB files to send to the selected Collection Master(s).

Table 85

Icon	Represents
	CAB files successfully sent to the Collection Master(s).
	CAB files not successfully sent to the Collection Master(s).
	CAB files in queue.
	CAB files being sent to the Collection Master(s).
	CAB files that were created prior to adding the Collection Master destination are marked as "Do not send." You have to select the CAB files explicitly to send to the Collection Master(s) by clicking Start.

Sending CAB file(s) to Collection Master(s)

This option helps you select Collection Master(s) and CAB file(s) that are to be sent to the selected Collection Master(s).

To send CAB file(s)

1 Click **Manage CAB** on the Collection Point Console.

EventTracker displays the Manage CAB Console.

Figure 439 Manage CAB console

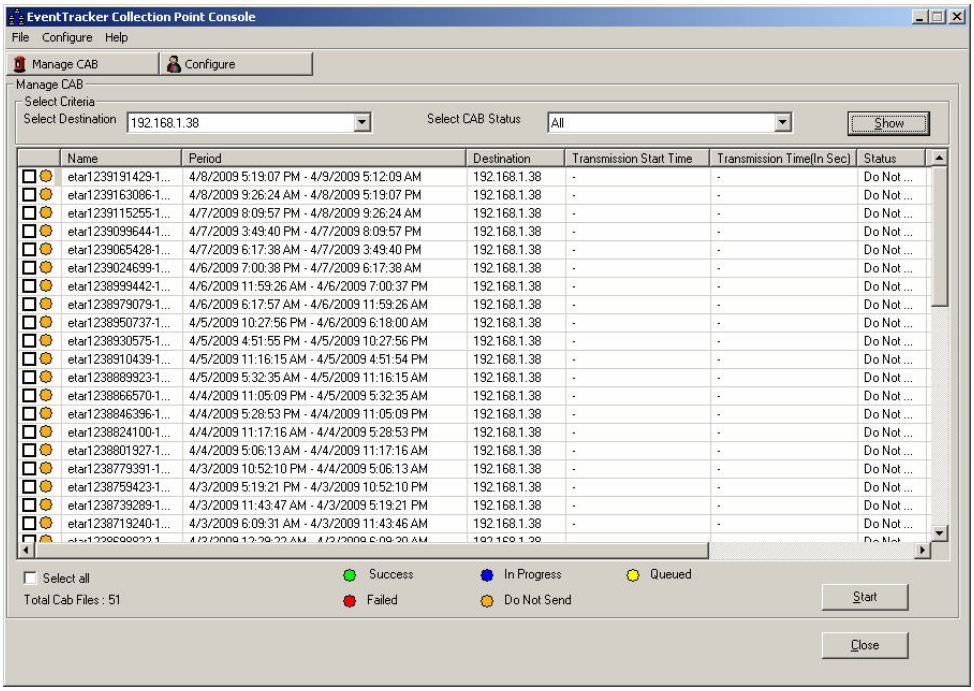


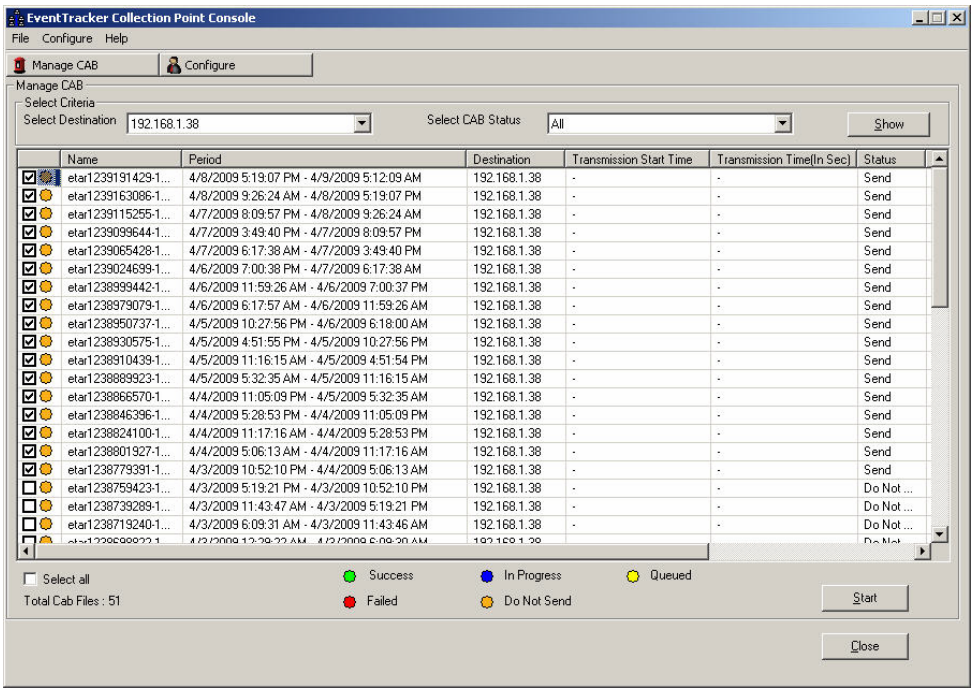
Table 86

Field	Description
Select Criteria	
Select Destination	Select Destination from the drop-down list. All configured Collection Masters are listed in this drop-down list.
Select CAB Status	Select the status of the CAB files from this drop-down list and then click **Show**. Available options are **All**, **Success**, **Failed, Do Not Send, In Progress** and **Queued**.
Select All	Select this check box to mark all the CAB files to send to the selected Collection Master(s).

2 Select the Destination from the **Select Destination** drop-down list. Default is All, which means Collection Point will send the selected CAB files to all the configured Collection Masters.

3 Select the CAB file(s) that you want to send to Collection Master.

Figure 440 Manage CAB console



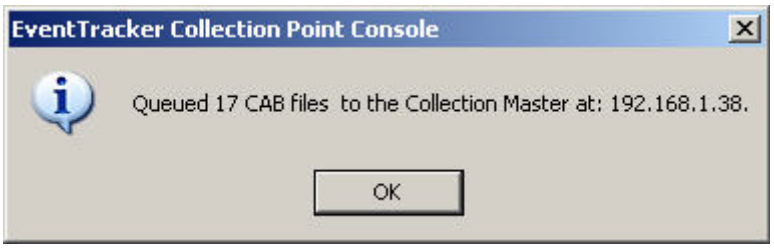
Note ¶

Select the **Select all** check box to send all the CAB files.

4 Click **Start**.

EventTracker displays the message box.

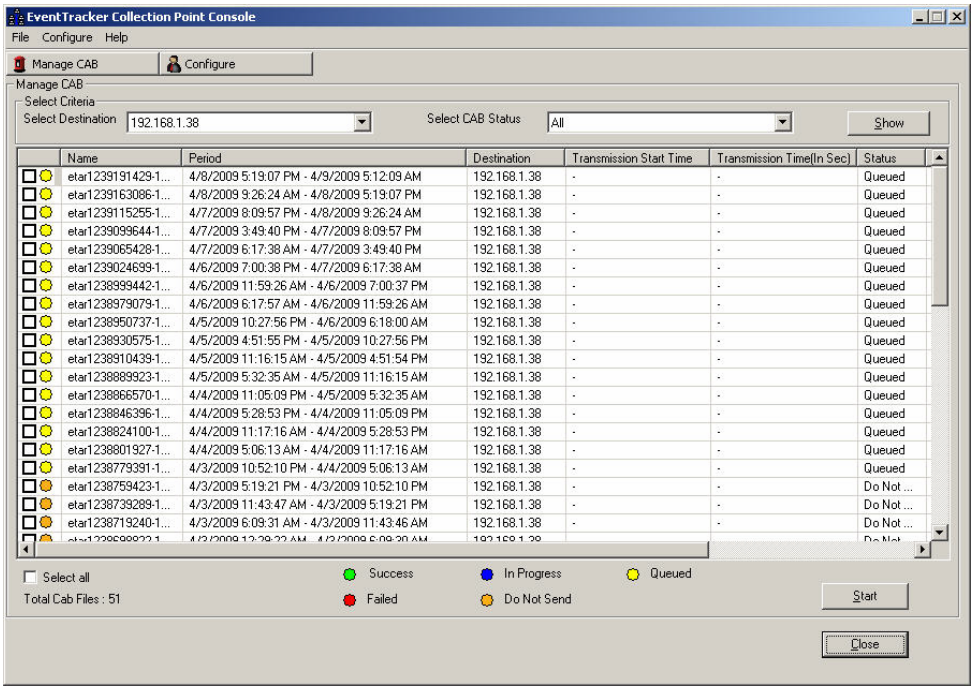
Figure 441 Collection Point Console message box



5 Click **OK**.

EventTracker displays the Manage CAB console with the new status of selected Cabs.

Figure 442 Manage CAB console



6 Select an appropriate option from the **Select CAB Status** drop-down list to view the status of CAB files.

When CAB files are sent successfully, EventTracker displays the Manage CAB console.

Figure 443 Manage CAB console

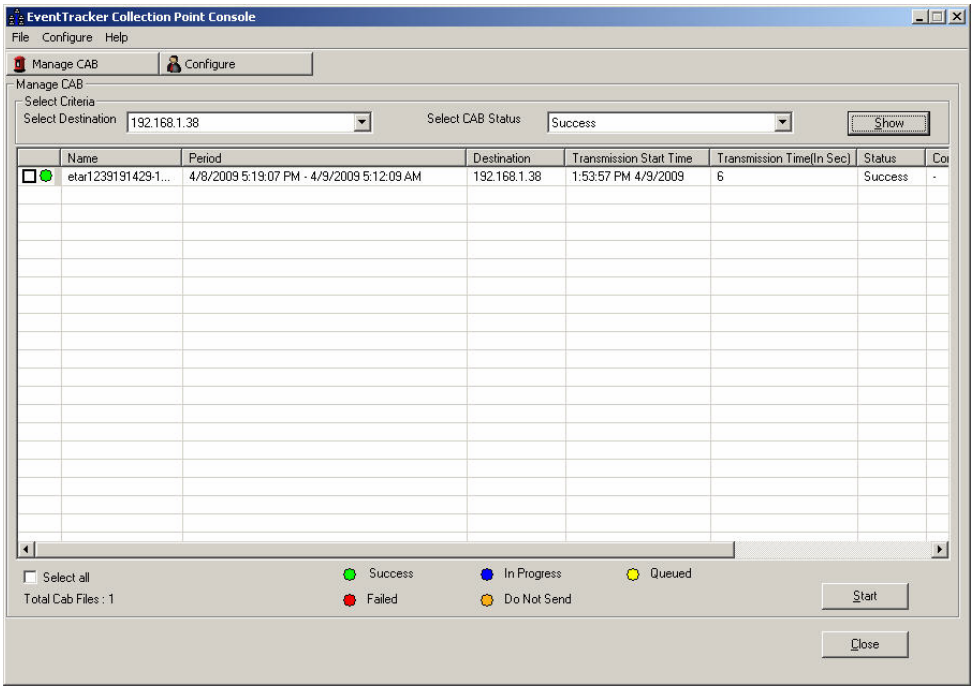
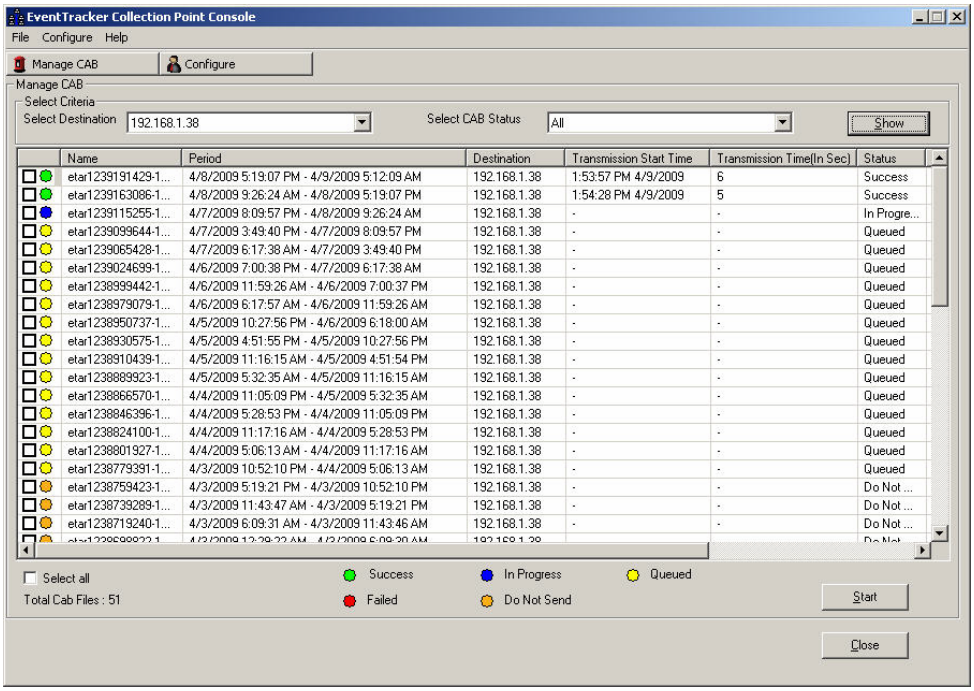
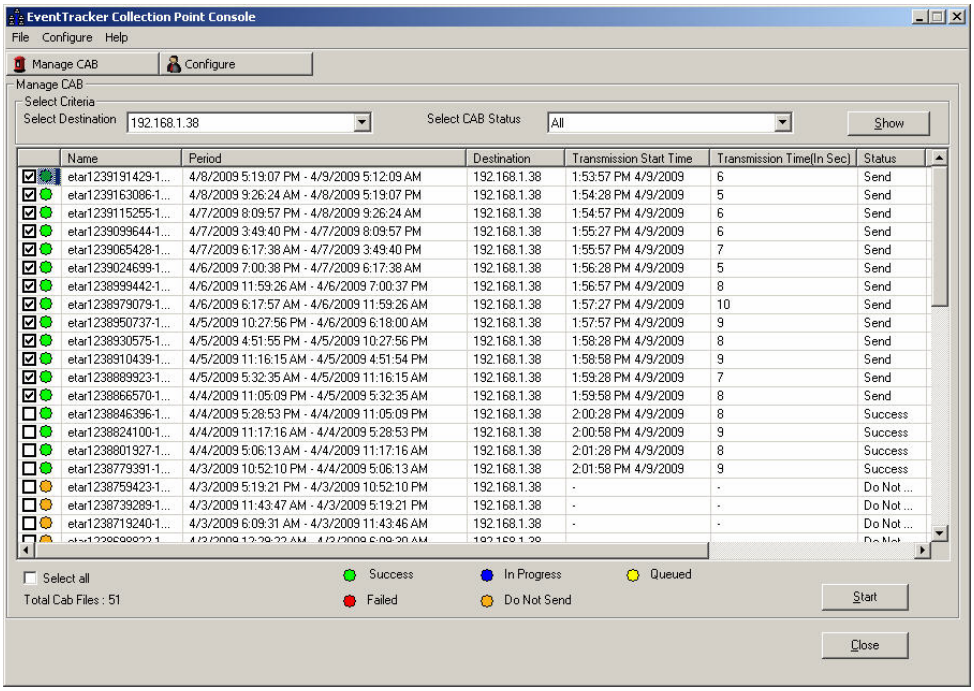


Figure 444 Manage CAB console



You can also resend the CAB files that are already sent to the Collection Master(s). EventTracker changes the status of the selected CAB files and displays the CAB Status console.

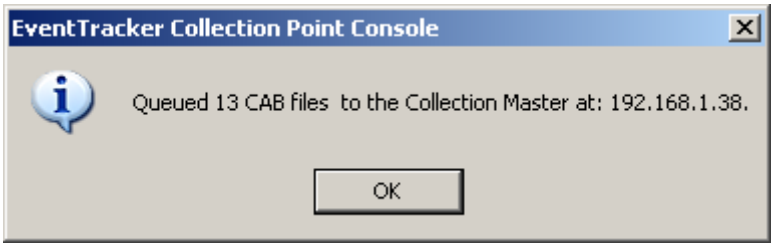
Figure 445 Manage CAB console



7 Click **Start**.

EventTracker displays the message box.

Figure 446 Collection Point Console message box



Collection Point resends the selected CAB files to the selected Collection Master(s).

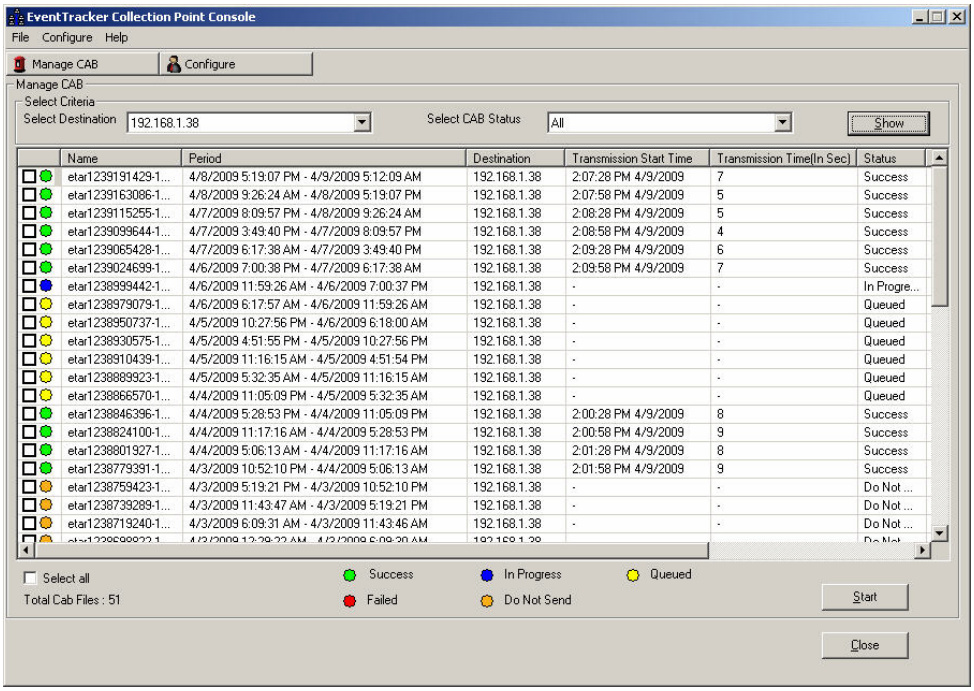
Note

When you resend a CAB file, Collection Master backs up the older one with the same name but appends timeticks. Timeticks is the time when the Collection Master received the new CAB.

For example CAB file **etar1238866570-14505.cab** is already sent and you have selected them to resend. Collection Master backs up the files received earlier with the same name but appends timeticks to the file name **etar1238866570-14505.cab_1239266608** where **1239266608** is timeticks.

EventTracker displays the CAB files with In Progress status with blue indicators.

Figure 447 Manage CAB console



Chapter 17
EventTracker Configuration Tracking

In this chapter, you will learn about:

- EventTracker Configuration Audit Tracking Events

EventTracker Configuration Tracking Events

EventTracker logs the following events when configuration changes are made to EventTracker Windows Agent, Custom Column (EventTracker & ELC), Report/Analysis (EventTracker & ELC), and Roles in ELC.

Table 87

Category	Description	Event ID
EventTracker: Agent configuration changes	ll events logged by EventTracker when any configuration changes made to the EventTracker Windows Agent.	3249
EventTracker: Custom column config changes	All events logged by EventTracker/EventLogCentral, when user adds a new custom column, modifies or deletes a custom column.	3286 - Addition of a custom column. 3287 - Modification of a custom column. 3288 - Deletion of a custom column.
EventTracker: Report/Analysis config changes	All events logged by EventTracker/EventLogCentral, when user adds a Report/Analysis, modifies or deletes a Report/Analysis (Scheduled, On-demand, Queued, Defined).	3283 - Addition of a Report/Analysis (Scheduled, On-demand, Queued, Defined). 3284 - Modification of a Report/Analysis (Scheduled, On-demand, Queued, Defined). 3285 - Deletion of a Report/Analysis (Scheduled, On-demand, Queued, Defined). 3289 - Modification of report saving options.
EventLogCentral: Role config changes	All events logged by EventLogCentral when user adds a new role, modifies or deletes a role.	3290 - Addition of a new role in EventLogCentral. 3291 - Modification of a role in EventLogCentral. 3292 - Deletion of a role in EventLogCentral.

Chapter 18
TrapTracker

TrapTracker is an integral component of EventTracker, which helps you monitor and manage critical traps emitted by network devices.

TrapTracker for Windows (TTW) consists of 2 components, the TTW Manager and a built-in MIB Compiler/Browser.

TTW Manager is the heart of the architecture. You should install the TTW Manager on the system where you require all SNMP Traps to be monitored. You can configure Alerts and Trap Severity. Alerts include E-mail, beep, console message and other custom notifications.

MIB Compiler/Browser is provided to compile Custom MIBS into the TTW system.

TrapTracker for Windows (TTW) console consists of the following options:

- **Alerts**: After the installation is completed, you can configure TTW to send you alerts, based on the type of events that are received. The types of Alerts supported are E-mail, beep, console message, and custom action.
- **Multiple Window View**: Displays multiple windows to view a distinct set of events. You can set the selection criteria for viewing events.

Chapter 19
Add-in Software Modules

In this chapter, you will learn about:

- WhatChanged
- StatusTracker
- EventLogCentral
- Solaris Agent

WhatChanged

This tool helps you understand the occurred changes on a computer's file system and registry and provides you with a lifeline to restore it back to a working configuration. WhatChanged architecture is completely centralized and provides you with the control to manage all systems on your network from one console.

WhatChanged console consists of the following options:

- **Snapshots**: After the installation is completed, WhatChanged initiates a snapshot that is called baseline snapshot. You can schedule the snapshots by using the configuration option. By default it is scheduled for 2 auto snapshots per day. You can change the timing and frequency.
- **Agent Installation / Distribution**: You can install WhatChanged Agents on any system that is present in any trusted domains. All Agents installed from a WhatChanged console can be managed from the WhatChanged console.
- **Full View/Change View**: In the Full View, WhatChanged console displays all the items in the file system and registry while highlighting only the changed items. In the Change View, WhatChanged console displays only the items that have undergone some changes.
- **Registry Restore/Undo Restore**: WhatChanged provides you with an option to make a comparison between the latest snapshot and any of the previous snapshots. After comparing them, you can restore any registry key to its older value. You can also undo the restore, in case the restoration was incorrect.
- **Reporting**: Reports are provided to identify the registry, file, and directory details. Reports are available in `.txt` format, and `excel` format. Change Reporter enables you to export reports to any popular standard.

StatusTracker

This tool helps you monitor the status of your IT resources and provides you various reports. You can make decisions based on the reports, to enhance the availability of your critical IT resources.

The StatusTracker console consists of the following options:

- **Managing Resources**: You can add resources through Web site, FTP Site, Manually, and IP Subnet. You can also modify and delete the existing resources.
- **Managing Groups**: You can create a group for the selected resources. You can also modify and delete the existing group.
- **Managing Alerts**: You can configure the alerts based on any change in resource status or any change in group status.

- **Reporting**: You can generate the report on Cost to Resource Availability, Resource Stability, Cost of Resource Downtime, and Resource Availability Summary.

EventLogCentral

EventLogCentral is a web-based user interface for EventTracker. ELC manages the event log data collected by EventTracker by consolidating events by groups, systems and event categories. You can generate on demand and schedule reports with the collected event data.

Evaluation and Purchase

To evaluate WhatChanged, EventTracker, and EventLogCentral, download the trial version from http://www.prismmicrosys.com/productDownloads.php

To purchase, contact us by E-mail at sales@prismmicrosys.com

Solaris Agent

EventTracker for Solaris C-2 provides administrators with a monitoring and reporting interface that provides one the most information rich sources of audit information from the UNIX kernel. Using the Basic Security Module (BSM), the system administrator now has access to kernel auditing events. Audit logs can be extremely valuable for operations, security, and auditors alike. EventTracker manages the central repository of log data events needed for proper incident investigation or to meet regulatory compliance. The platform provides insights into the actions and behaviors of users and systems. This information can be used to detect insider threats, security violations, and other dangerous behavior patterns.

Benefits of Solaris Agent

- Convert BSM binary data into meaningful events
- Real-time user-defined alerts
- Event Correlation engine
- Secure event archival
- Access to EventTracker database and EventVault for reporting

Purchase

To purchase Solaris Agent, contact us by E-mail at sales@prismmicrosys.com

Appendix – HIPAA

HIPAA Compliance Reports

The Health Insurance Portability And Accountability (HIPAA) regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use of disclosure of the information.

As part of the requirements, HIPAA states that a security management process must exist in order to protect against "attempted or successful unauthorized access, use, disclosure, modification or modification with system operations." The organization must be able to monitor, report and alert on attempted or successful access to systems and application that contain sensitive patient information.

EventTracker provides the following reports to help comply with the HIPAA regulations:

User Logon report

HIPAA requirements (164.308 (a)(5) – log-in/log-out monitoring) states that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

HIPAA requirements clearly states that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

HIPAA requirements (164.308 (a)(3) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

Appendix – SOX

Sarbanes – Oxley Compliance Reports

Section 404 of the Sarbanes – Oxley (SOX) act describes specific regulations requires for publicly traded companies to document the management's "Assessment of Internal Controls" over security processes.

The standard requires that a security management process must exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification or interference with system operations. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information.

ELC provides the following reports to help comply with the SOX regulations:

User Logoff report

SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

User Logon report

SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report

The security logon failure includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

SOX requirements (Sec (a)(4)(C) and (D) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

Security Log Archiving Utility

Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.

Track Account management changes

Significant changes in the internal controls sec 302 (a)(6). Changes in the security configuration settings such as adding or removing a user account to an administrative group. These changes can be tracked by analyzing event logs.

Track Audit policy changes

Comply with internal controls sec 302 (a)(5) by tracking the event logs for any changes in the security audit policy.

Track individual user actions

Comply with internal controls sec 302 (a)(5) by auditing user activity.

Track application access

Comply with internal controls sec 302 (a)(5) by tracking applications process.

Track directory / file access

Comply with internal controls sec 302 (a)(5) for any access violation.

Appendix – GLBA

GLBA Compliance Reports

Section 501 of the GLBA documents specific regulations require for financial institutions to protect “non-public personal information.”

As part of the GLBA requirements, it is necessary that a security management process exist in order to protect against attempted or successful unauthorized address, use, disclosure, modification or interference of customer records. The organization must be able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive customer information.

User Logon report

GLBA Compliance requirements state that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

GLBA requirements state that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

GLBA requirements (review and audit access logs) call for procedures to regularly review records of information system activity such as audit logs.

Appendix – Security Reports

Security Reports

Successful and failed file access

Auditors are generally concerned with knowing who did what, and when. Monitoring file access can provide that information. This will be especially useful as companies attempt to comply with internal policies and industry regulations.

Successful logons preceded by failed logons

Multiple failed logins, followed by a successful login could indicate a successful breach by a hacker.

Audit log cleared events by user

A successful hacker will attempt to remove any trace of their attack. Their attempts to clear the audit logs are captured and can be displayed with this report.

Invalid logons by date

Allows you to identify days of heavy invalid logins. Many invalid logins over a weekend could indicate an attempt to penetrate the network.

Daily reboot statistics

Daily reboot statistics can help system administrators identify systems that might be having problems.

CPU load peaks by computers

CPU load peaks can indicate a system that is either configured incorrectly or one that is simply overworked. This can allow the system administrator to identify the system having problems and either fix the issues or transfer some of the workload (or justify new hardware).

Account usage outside of normal hours

This report can identify those accounts that are being used outside of normal (definable) hours of operations. Users occasionally work late, but frequent account usage after hours can indicate a security breach.

Audit policy history

Tracking audit policy on enterprise systems is a key function for security auditors. The "Audit Policy History" report will show each systems audit policy for ach date it was collected. This way compliance to the audit policy is documented and can be tracked.

Accounts that were never logged on

Part of an administrator's job is to deal with the clutter that collects in the NT4 SAM or Active Directory – or perhaps better stated, preventing it entirely. One of the more common sources of this clutter is redundant user accounts. In an effort to provide efficient service, those tasked with account creation often create new user accounts ahead of time for new employees or contractors. That way, when the new employee or contractor arrives, they can login and start to work immediately. In some organizations, this may mean dozens of accounts. Inevitable, job offers are declined or contractors' start dates postponed. The result is accounts that exist but have never been used. These accounts potentially represent a security risk because

1. They usually have a well-known default password ser and
2. They may already have been placed in security groups pertaining to their job function.

An unscrupulous individual could login as the new account, set password to one of their own choosing and gain access to sensitive data by way of the accounts' group memberships. The "Accounts that were never logged on" report can highlight these risky redundant accounts. Armed with this information follow-up e-mails can then sent to the appropriate managers to determine what has transpired with the individuals for whom these accounts were created – i.e. did they really start work yet or not. Once the status of the employees is known, these accounts may then be disabled or deleted as required.

Administrative Access to Computers

Administrative access is required to perform many common tasks on workstations and servers. Such tasks include stopping and starting services, installing software and creating local groups for data permission. Care needs to be taken in the assignment of local administrative rights as clearly, an account with this right has a quite ranging ability to modify applications on SQL or IIS for example inappropriately assigned administrative access could lead to outages of business line applications.

On the other side of this equation are enterprising power users who will sometimes go out of their way to block administrators' legitimate access to their machines. These situations cause innumerable problems when it comes time to do remote managements, hardware and software inventory, software rollouts and even access control list updating. In either case, administrators need to get a sense of who has local administrative authority on workstations and servers in their environment. The "Administrator Access by Computer" report can quickly provide this invaluable information.

File Access by User

Ensuring that appropriate permission is set on sensitive data is one side of the data security coin. The other is the process of auditing who is using the permissioned resources and when. There are times when it is important to know who the last person was to use their authorized access a resource. It is just as important to know if someone is trying to access a resource that he or she does not have access to.

Take the example of a spreadsheet containing salary information. "Mary Hart" works in human resources and is authorized to access this information. E\ach time she accesses the file, if auditing is enabled, this access will be recorded to Windows' Event Logs as successful access. On the other hand, "George hogan" is an employee in the mailroom, with some time on his hands. He spends this time browsing the network. Since he is part of the company' Administration Department, he has visibility of the department's shared files. He may be able to see a folder called "Payroll Info" – when he tries to access this folder, however, he will receive the message "Access Denied." The fact that he unsuccessfully tried to access this folder will also be recorded to the Event Logs as a "failed file access."

The event log information described about is another distributed data source. Each files server maintains its own store of information on who accessed what file on that server and when. The challenge is to consolidate this information into one location and extract the most relevant transactions.

Hot fixes by Computer

Microsoft releases hot fixes on an almost weekly basis to remedy critical technical and security problems with the operating system. Clearly, these problems are considered serious enough that they might significantly disrupt a customer's business if not repaired. This puts pressure on administrators to keep close track of which hot fixes are installed on servers and workstations – an essential but potentially time-consuming task. Being able to poll computers on a scheduled (e.g. weekly) basis to verify which hot fixes they have installed means having on fewer balls to juggle.

Reporter's Hot Fixes by Computer report obviates the need to use a second tool to the collected hot fix information. The report interrogates the Registry of each workstation and server on the network to determine which hot fixes are installed. Like all of Reporter's reports, this process can be scheduled at whatever interval the administrator deems appropriate. This way, the hot fixes check becomes part of the administrator's standard list of scheduled audit reports. Frequent collection ensures that the most current information is always at hand.

Last logon by Domain Controller

As previously noted, identifying redundant user accounts is an important step towards achieving a secure network. We previously discussed the use of the "user never logged on report" to highlight accounts that were created but have never been used. Another more frequent and common scenario is an employee or contractor leaves the organizations but IT is not notified. Though policies may be in place that stipulate that the accounts of departed staff are to be disabled and eventually deleted – if IT doesn't

know that someone had left they really have no way of knowing which accounts need to disabled on a given day.

One indication of whether an account is being used or not is the "last logon time." Each time a user enters their username and password (either at logon time or as part of unlocking their workstation), a logon transaction is recorded and the time of that transaction is stamped on to that user's account. For the most part, if an account's last logon time is more than 2 to 3 weeks in the past (this takes into account possible employee vacations, training courses or travel), this is a good indication that the employee is not working with the company.

Reporter's "Last Logon by Domain Controller" report is an authoritative source of users' last logon times. The report polls all domain controllers (DCs) for the last logon seen by that DC for each user and then calculates the most recent time for insertion into the report. As part of a regular security audit process, this report could be scheduled to run on at least a weekly basis. Armed with this report, follow-up e-mails can then be sent to the appropriate managers to determine what has transpired with the employees whose accounts appear in the report – i.e. have these staff left the company or are they on some extended leave. Once the status of the employee is known, these accounts may then be disabled or deleted as required.

User Account Locked Out

User account lockouts occur when a user incorrectly enters password several times in succession. In most organizations, a user who enters their password incorrectly three times will have their account locked out (i.e. be barred from accessing the network) for some defined time period (e.g. 15minutes) or possibly, indefinitely.

Frequent user account lockouts can result from clumsy or forgetful users but they may also be an indication of some trying to gain unauthorized access to the network using their own or someone else's account. Like file and resource access, account lockouts are recorded in Windows' Event logs of each server that authenticates user access. Once again, the challenge is to pull this information together.

Reporter's User Account Locked Out report extracts lock out events from all the data collected from servers across the company effectively mining out the transactions that might indicate suspicious activity. As part of the regular audit process, it would be advisable to schedule the execution of this report in the early morning hours just prior to start of business (e.g. at 6 a.m.).

This would highlight to the administrator or security officer all accounts that were locked during the overnight period. Careful review of the report could help to determine if sleepy users caused the lockouts or someone trying hack into the network at night. Another business use of this information can be to provide some insight into Help Desk call volumes. If, on a given day, there was a large increase in calls to the Help Desk, a quick perusal of the account lockout report might provide at least part of the explanation for the increase.

Appendix – BASEL II

BASEL II

In the financial services industry, nothing is more than the trust of customers, shareholders, partners and regulators. The risk management officer's primary task is to ensure trust is sustained through a systematic risk management program.

BASEL II defines operational risk, one of the pillars of the Accord, as "the risk of direct or indirect loss resulting from the inadequate or failed internal process or systems or from external events."

If your company eventually intends to adopt the Advanced Measurement Approach (AMA), then you are required to measure aspects of operational risk, such as IT security.

Appendix – FISMA

FISMA

FISMA requires detailed annual E-Government security reports of all federal agencies. As to fulfill FISMA requirements, the agencies should implement the FISMA requirements and transmit the corresponding reports to Office of Management and Budget (OMB) by October of each year. According to the sections **FISMA Sec. 3505** and **FISMA Sec. 3544**, the transmitted reports should summarize the following requirements to comply with FISMA.

FISMA Sec. 3505

Sec.3505.(c)(1) - Maintenance and results of major federal information systems or applications inventory security of the agency.

Sec.3505.(c)(2) - Inventory of networks interfaces not only within the agency, but also the network of other agencies or contractors working under the agency.

FISMA Sec. 3544

Sec.3544.(a)(1)(A)(i) - Information security protection against unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems of the agency.

Sec.3544.(a)(1)(A)(ii) - Information security against unauthorized usage risks of the contractor or other organizations working on behalf of the agency.

Sec.3544.(a)(1)(A)(ii) - The responsibility of the head while the major federal systems operated either by the agency or by the contractor and other agencies under the agency.

Sec.3544. (b) - Integrity, authenticity, availability of the systems supporting the agency operations and assets.

Sec.3544. (b)(2)(C) - Detailed reporting on the existing risks and remedial actions. Effectiveness of Information Assurance program and progress in remedial plans and actions.

Sec.3544. (b)(2)(D) – Periodical risk management reporting. Accurate report on the current FISMA compliance status. Annual information on security training and Internet security training for the agency personnel and also the contractor.

Appendix – PCI DSS

PCI DSS

PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or they risk losing the ability to process credit card payments.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Glossary

Term	Description
Advanced Report	The report for any period for which events have been collected based on the selection criteria. You can generate Summary Report and Detailed Report.
Agent Configuration	Process of configuring the system for reporting to multiple managers, to filter events, to monitor services, software installations, processes, system health, and to archive the events database.
Alert Configuration	Process of configuring alert notifications in the form of Sound, E-mail, Console message or any Custom action.
Alerts	A feature that instructs programs that notify timely information about the events.
Analyzing Event Traffic	The process to analyze the event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.
Audible Alert	A feature that instructs programs that usually notifies information by sound.
Auto Discover Mode	Process of adding computers from your network automatically.
Auto Scrolling	Process of selecting the latest event automatically in the content area.
Change Management	The process that enables the user to monitor, analyze, understand, and recover from change.
Console Message Alert	A feature that instructs programs that usually notifies information to the selected machine.
CPU Performance	A term used to monitor the CPU performance.
Custom Alert	A feature that instructs programs to execute custom action on receipt of an event.
Disk Space Usage	A term used to monitor the disk space usage.
E-mail Alert	A feature that instructs programs that usually notifies information by E-mail.
Log Analysis	Process of analyzing the event details by setting criteria such as date range, time range, rule, and computer.
Event Filtering	Process of filtering the events that are not important. Monitoring unimportant events cause the database to occupy more disk space.

Term	Description
Event History	The report for the selected period for which events have been collected based on the setting criteria.
Event Information	A window pane that displays the summary of event details in the EventTracker Management console.
Event Logs	A type of event message. The event logs are recorded whenever certain events occur, such as services starting and stopping, or users logging on and off and accessing resources.
Event Monitoring	A window pane that displays the real-time event information in the EventTracker Management console.
EventTracker	An application that can be used to centrally monitor, analyze, manage events being emitted by Windows NT/2000/XP, UNIX systems, and SNMP enabled devices.
EventBox	An archived event data file. You can create an EventBox by using EventVault Warehouse Manager console.
EventTracker Statistics	The process to view the summary of event statistics such as Total events received, Total alerts received, Total systems monitored, and so on.
EventVault	The console used to archive the events from EventTracker database. EventVault can operate in Automatic Archival and EventBox on demand methods.
Exclude List	The process to configure the network connections that need not to be monitored.
Filters	The process to filter out events that you do not want to monitor.
Include List	The process to configure the network connections to monitor. Include list Network connections always override the Exclude list Network connections.
IP Subnet	A 32-bit address used to identify a node on an IP internet. The address is typically represented with a decimal value of each octet separated by a period. For example: 192.168.7.27.
Knowledge Base	A Web site containing information about Windows events and custom EventTracker events.
Log Backup	A backup that copies event logs automatically in the EventTracker Agent directory whenever the event logs are full.

Term	Description
Logfiles	The process to monitor textual log files such as SQL or ISA logs, created by any vendor. You can also configure the strings to search. If any record matching the search string is found, an event will be generated.
Manager Configuration	Process of configuring parameters of Acknowledge Events time limit, Maximum Events view limit, Purge Time limit, Ping Frequency and connected server name.
Memory Usage	A term used to monitor the memory usage.
Monitor Syslog	The process to monitor Syslog being sent by an UNIX system.
Quick Statistics	The process to view the summary of event statistics such as Total events received, Total alerts received, Total systems monitored, and so on.
SNMP Event Manager	An application called TrapTracker used to monitor and manage critical traps emitted by network devices in your enterprise.
SNMP Traps	The process to receive trap messages generated by local or remote SNMP agents and forwards the messages to third party vendor software such as an NOC.
StatusTracker	An application used to monitor the status of your IT resources and provides you various reports.
Syslog Receiver	The process to set the SYSLOG receiver. After setting this option, the Manager will receive any SYSLOG being sent by an UNIX system.
System Information	The process to collect and view the system configuration information. You can view the information of System Summary, Hardware Resources, Components, Software Environment, Internet Settings, and Applications.
System Manager	A console helps you to manage groups, systems, and Agents.
System Performance	The process to monitor the system performance in graph, histogram, or report form.
System Statistics	A window that displays the system statistics in EventTracker Management console.
TCP	Transmission Control Protocol. TCP is responsible for verifying the correct delivery of data from Agent to server. TCP adds support to detect errors or lost data and to trigger transmission until the data is correctly and complete received.

Term	Description
UDP	User Datagram Protocol. A connectionless protocol that, like TCP, runs on top IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network.
WhatChanged	An application that used to track the occurred changes on a computer's file system and registry and provides you with a lifeline to restore it back to a working configuration.

Index

A

About x
- Available features 31
- License Info 32
- License usage 31
- Patch Info 32
- System Info 33

Add-in Software Modules
- EventLogCentral 454
- Solaris Agent 454
- StatusTracker 453
- WhatChanged 453

Agent
- advanced filters 227
- applying settings 286
- backup configuration 289
- basic configuration 214
- changing account 204
- event delivery mode 218
- filtering events 221
- filtering events with exception 225
- high performance mode 231
- Installing 182
- multiple destinations 215
- pre-installation procedures 182
- protecting configuration 290
- Removing client components 198
- SID translation 230
- starting client service 204
- switching modes 200
- system health 232
- Uninstalling 191
- Upgrading 194
- viewing status 204

Agent Management Tool 292
- accessing 292

Agent service status
- all 295
- group 294
- system 293

Agent service version
- all 298
- group 297
- system 297

Agentless Monitoring 304
- adding 304
- editing admin account 310

Alert Actions
- edit 123
- predefined Alerts 129

Alerts 85
- configure 85
- Dashboard 130
- delete 104
- manager side actions 105
- modify 103

Auto Discover mode
- Removing computers 155

Auto scrolling 61

C

Category Groups 348
- adding categories 352
- creating 348
- deleting 358
- managing 358
- modifying 357

Choosing Columns 41

Collection Master
- CAB status 408
- Collection Point details 407
- configuring Alerts 432
- configuring port 411
- deleting CABs 428
- deleting Collection Point details 430
- merging Collection Points 412, 416
- requesting CABs 424
- starting 406

Collection Point
- adding Collection Masters 436
- deleting Collection Master settings 441
- editing Collection Master settings 440
- sending CABs 443
- starting 435
- viewing CAB status 442

Collection Point model 401
- scalability 401
- scenarios 402

Command line mode
- multiple systems 301

Command Line Mode
- deploy 298
- install on single system 299

parameters 298
uninstall from single system 301
Compliance
BASEL 464
FISMA 465
GLBA 459
HIPAA 456
PCI DSS 466
Security Reports 460
SOX 457
Computer
removing 155
Configuration Tracking 450
agent 450
custom column 450
reports/analyses 450
roles 450
Configure
Alert notification tracking 77
Audible Alerts 105
Console message Alerts 112
correlation receiver 76
Custom action 121
DLA 76
E-mail Alerts 108
Forwarding events as SNMP Traps 116, 118
Knowledge Base 64
Manager to alert suspicious network activity 81
purge Alert events cache 77
remedial actions 79
RSS Alerts 114
show only active Alert events 78
SYSLOG receiver 65
Window view limit (Console) 64
Control Panel
Collection Master 21
Collection Point 22
Standard 23

D

Diagnostic & Support 37
Discover Modes 147
Auto 147
Manual 147
Duplicate Alerts 80
suppress 80

E

Event Categories
Alerts 370
creating 359
deleting 369
modifying 365
Event Details
deleting 369
Event Traffic Analysis 331
category 332
correlate 333
custom 335
event id 333
Event-O-Meter 27
EventTracker
about 14
control panel 20
icons 28
management console 25
services and ports 16
starting 18
EventTracker Components
EventVault Warehouse Manager 35
Knowledge Base 37
System Manager 33
EventVault
appending CABs 323
backup 317
configuring 315
deleting EventBox 321
extracting EventBox 321
moving CABs 322
saving EventBox information 319
verifying EventBox integrity 320
viewing CABs 314
Export
Alerts 377
Categories 374
Domains 379
Filters 376
RSS Feeds 384
Scheduled reports 382
Systems 380

F

Filtering Events
advanced filters 228
Filtering events from view 43
configure event filters 44
deleting event filters 51

event filters with exception 51
modify filter settings 50
FISMA
sec 3505 465
sec 3544 465

G

GLBA
audit logs access 459
logon failure 459
user logoff 459
user logon 459

H

HIPAA
audit logs access 456
logon failure 456
user logoff 456
user logon 456

I

Import
Alerts 390
Categories 385
Domains 392
Filters 387
RSS Feeds 397
Scheduled reports 396
Systems 394

L

Log Search 331
Logical System Groups 163
IP Subnet 167
Manual selection 169
System Type 163

M

Maitenance Tools
Archive Indexer 140
DB Compaction 142
Manual Mode
Adding a group of computers 150
Adding a group of computers - IP subnet 152
Adding a single computer 148
Manula Mode
Removing computers 157
Monitoring
applications 238
Check Point logs 257
EVT Logfiles 212
excluding network connections 267
filtered processes 282
filtering applications not to monitor 240
filtering applications to monitor 241
filtering services not to monitor 244
including network connections 271
log backup 283
logfiles 245
network connections 264
processes 280
searcing strings 255
services 242
suspicious connections 273
Trusted List 274
VMware logs 261

R

Reloading the Navigation Pane 58
Remedial Action 126
Removing unmanaged systems . 158
Restarting Agent service
all 296
group 296
system 295
RSS Feeds 133
adding 133
deleting 136

S

Scheduler service 313
Collection Master 314
Collection Point 314
Search Based Console 41
Security Reports
account usage outside of normal hours 460
accounts that were never logged on 461
administrative access to computers 461
audit log cleared events by user ... 460
audit policy history 461

CPU load peaks by computers 460
daily reboot statistics 460
file access by user 462
hot fixes by computer..... 462
invalid logons by date 460
last logon by Domain Controller... 462
successful and failed file access.. 460
successful and logons preceded by failed logons..... 460
user account locked out..... 463
SOX
account management changes.... 458
application access 458
audit logs access 457
audit policy changes 458
directory / file access 458
individual user actions 458
logon failure 457
security log archiving utility 457
user logoff..... 457
user logon..... 457
Suspicious Connections 273
System Report..... 207
all 209
managed system 208
unmanaged system 209

T

TrapTracker 451
Trusted List
adding programs.....278
firewall exceptions 279

U

Understaing filers and filter exceptions..... 55
Upgrade..... 29
USB 235
User Activity..... 340

V

Viewing and editing Alert details .. 56
show alert rule 56
Virtual Collection Points 66
architecture.....66
configuring EventTracker Receiver.67
forwarding raw syslog messages....70
syslogs.....68
Windows events 71
Vista Agent 209
prerequisites.....210
VistaAgent
event consumers 210
event logs and channels.....210
event publisher 209
EVTX 212